Security Escort

SE2000 Series

BOSCH

en Technical Reference Manual

Table of contents

1 Copyright and warranty

1.1 Trademarks

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

1.2 Software license agreement

Security Escort's Central Control software for Microsoft® Windows®.

Notice!

This software relates to security. Access should be limited to authorized individuals. This software contains provisions for setting security passwords. Appropriate security levels should be established and passwords should be set before allowing operating personnel access to this software. The original disk should be safeguarded against unauthorized use. In addition, security/fire controls contain passwords to prevent unauthorized access; these passwords must also be set and their identity carefully safeguarded.

Please read the following license agreement prior to installing and operating the software. Do not install this software unless you agree to the following terms:

You MAY

- Use the Security Escort program only on a single Security Escort system, with a single master computer, a single optional slave computer, and only the number of workstations originally factory programmed into the software key.
- This program can be used without a software key only for demo purposes. In no case can this program be used on a live system without an authorized software key.
- Copy the program into another computer only for backup purposes in support of your use of the program on one Security Escort system.

You may NOT

- Transfer this program or license to any other party without the express written approval of Bosch Security Systems.

1.3 Limited warranty

Bosch Security Systems warrants that the program will substantially conform to the published specifications and documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. Bosch Security Systems also warrants that the magnetic media on which the program is distributed and the documentation are free of defects in materials and workmanship. No Bosch Security Systems dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty, oral, or written. Except as specifically provided above, Bosch Security Systems makes no warranty or representation, either express or implied, with respect to this program or documentation, including their quality, performance, merchantability, or fitness for a particular purpose.

1.4 Remedy

Bosch Security Systems will replace defective media or documentation, or correct substantial program errors at no charge, provided you return the item with proof of purchase to Bosch Security Systems within 90 days of the date of delivery. If Bosch Security Systems is unable to replace defective media or documentation, or correct substantial program errors, Bosch Security Systems will refund the license fee. These are your sole remedies for any breach of warranty.

Because programs are inherently complex and may not be completely free of errors, you are advised to verify your work. In no event will Bosch Security Systems be liable for direct, indirect, incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, Bosch Security Systems is not responsible for any costs including, but not limited to, those incurred as a result of lost profits or revenue, loss of use of the computer programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. Bosch Security Systems does not represent that the licensed programs may not be compromised or circumvented. In no case shall Bosch Security Systems liability exceed the amount of the license.

Some states do not allow the exclusion or limitation of implied warranties, or limitation of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Bosch Security Systems retains all rights not expressly granted. Nothing in this license constitutes a waiver of Bosch Security Systems rights under the U.S. Copyright laws or any other Federal or state law.

Should you have any questions concerning this license, write to:

Bosch Security Systems
130 Perinton Parkway,
Fairport, New York 14450

Robert Bosch Security Solutions Pte Ltd
11 Bishan Street 21
Singapore 573943

2 Security Escort system architecture

2.1 System overview

The Security Escort System consists of five basic components: transmitters, receivers, alert units, transponders, and the Central Console.

The transmitter is a miniature, radio transmitter, used to transmit either a distress or a test signal. The receivers are located throughout a protected area, and detect the radio transmissions from transmitters. Alert units are siren/strobe units activated in the event of an alarm. Transponders are devices that control groups of receivers and alert units, connected to them by wire. Each transponder relays alarm and test signals from its receivers to the central console. In addition, the transponder tests for device and wiring faults, and transmits problem conditions to the central console. The Central Console consists of a computer (the master computer), an optional backup computer (the slave computer). Up to eight optional workstation computers can be used to receive alarm and trouble signals from the transponders, analyze the signals, activate strobes and sirens on the alert units, and produce a display for the security dispatcher. Each of these system elements is described in further detail below.

2.2 System components

2.2.1 Transmitter

There are several types of transmitters for personal use; those normally assigned to system subscribers, one for security personnel, and one for maintenance personnel. Each transmitter type serves a different purpose. All versions of transmitters for personal use produce alarm and test transmissions.

Subscriber transmitter

Each transmitter contains a unique code, which is associated with the subscriber at the time the transmitter is assigned. In the event of an emergency, press and hold the alarm button(s) for 1 sec. to produce an alarm (see your transmitter user manual). Optionally, within approximately 2 sec., the sounders in a nearby receiver activate, as well as the strobes and sirens on nearby alert units.

The transmitters have a second feature, the test mode. When the user is indoors, in sight of an interior receiver or outdoors, in sight of an alert unit, pressing the test sequence performs a test (see your transmitter *User's Manual*). If the test is successful, a small green light flashes on the interior receiver, or the strobe on an alert unit flashes briefly. There is no response at all if the test fails. If the test fails, the user should try again. If there is still no response, the user should contact the security office as soon as possible. Every successful test is recorded in the **Subscriber Database** in the Central Console software and optionally printed on the hardcopy printer. The **Subscriber Database** contains all of the information relating to each subscriber, including the date and time of the most recent test transmission. It is possible to search the **Subscriber Database** for individuals who have not performed tests for a specified period of time.

Security transmitter

The security transmitters are unique in the way that both tests and alarms are processed. Outwardly, security transmitters perform in the same manner as normal transmitters during testing. That is, strobes flash on alert units and green lights flash on receivers to confirm a successful test. However, when a security transmitter is tested within close proximity of a receiver, the Central Console records not only the user identity, and the date and time (as with a normal user test) but also the location of the officer at the time of the test. These tests are designated by the term security test on the printout at the Central Console and provide a convenient means of recording security patrols. (To protect user privacy, location information is not printed out for regular subscribers during tests.)

The security transmitters also differ in the way that alarms are managed. Unlike regular transmitters, no sound is emitted from the transmitter itself, no horns are activated on receivers, and no strobes or sirens are activated.

The Central Console in the security office sounds an alert tone and displays the alarm as usual except for a yellow background and text advising that the event is a silent alarm from a security officer. This allows security personnel to call for assistance without attracting unwanted attention.

Maintenance transmitter

The maintenance transmitter is used exclusively for system set-up and diagnosis. Maintenance alarms are used during the system set-up to verify that a receiver is functioning and is properly identified in the **Transponder Database**. The maintenance alarm is also used to measure the received signal strength of the receivers from any location within the protected area. The Central Console distinguishes the maintenance transmitter by its unique coded message and produces a printout of the signal strengths reported by receivers on each transponder.

In the test mode, the maintenance transmitter behaves like a normal subscriber transmitter except that the Central Console does not verify the user ID portion of the transmitted code. Unlike the subscriber transmitters, all maintenance transmitters are assumed to be valid.

Point transmitter

The point transmitter is used to protect assets, not people. It has a magnetic reed switch and a supervised loop that reports both open and shorted states. The software can be programmed to report alarms and troubles on any of these conditions going off normal with unique text identifying the condition. These transmitters are supervised and also optionally support the alarm follower.

2.2.2 Receiver

The receivers are located throughout the protected area, including building interiors. Inside buildings, the spacing of these devices depends on the building construction and the locating precision required. Outdoors, spacing depends on terrain and foliage conditions and building obstructions. The procedure for location of receivers is contained in the Security Escort *Hardware Installation Manual*.

Each receiver contains a radio receiver to detect the transmissions from transmitters, and microcomputers to decode and interpret the received test and alarm messages. In addition, the microcomputers monitor to detect tampering, and report such conditions to the transponder.

Each receiver contains a sounder similar to those in self-contained smoke detectors. These sounders are optionally activated if the receiver has detected an alarm transmission.

Indoor receivers are typically mounted on inside walls. They are housed in small beige, rectangular units. Indoor receivers have one red and one green light. The green light is used to indicate a successful test of a transmitter. The red light is only illuminated during certain system tests and during alarms.

Outdoor receivers are contained in small weatherproof boxes typically mounted on the sides of buildings and on light posts. Outdoor receivers do not have the visible red and green LED’s. Outdoors, the strobe lights on the alert units flash to acknowledge successful tests.

In addition to its radio receiver, each receiver also contains a transmitter functionally similar to the hand held transmitters. This transmitter can be commanded by the Central Console to transmit a test message to other nearby receivers. This buddy checking is performed periodically to verify that the receiver sections of all receiver units are functioning satisfactorily.

2.2.3 Alert unit

An alert unit consists of two components: a self-contained strobe/siren unit and an electronic driver unit. The latter may be housed in either a metal indoor enclosure or an outdoor enclosure (similar to the outdoor receiver enclosure), depending on the application. The strobe siren units are always mounted in outdoor locations. In addition to the function of attracting attention in the event of an emergency, the strobe unit is used to acknowledge a successful test of a transmitter.

The alert unit has back-up battery power in addition to AC power. The alert unit driver contains a microprocessor, which communicates with the transponder for strobe and siren commands, status reports, and trouble indications. The troubles monitored are tamper, loss of AC power, and low battery.

2.2.4 Transponder

The transponder is a device controller for up to 64 devices; any combination of receivers and alert units. The devices are connected to the transponder by means of 8 four wire multiplex busses: two wires for power and two wires for data. Each bus is capable of supporting up to 8 devices. The Security Escort System supports up to 255 transponders.

Each receiver and alert unit is identified to its transponder by a multiplex address that is set during system installation using a multi-position switch on the receiver or alert unit circuit board. Transponders communicate on the data bus with individual multiplex devices by issuing commands, which contain the receiver or alert unit’s multiplex address. Note that a given transponder may have up to eight devices with the same binary multiplex address, one on each bus. Thus, the complete identification of a particular device must include the transponder with which it is associated (1 to 255), the bus on which it is located (0 to 7), and its binary multiplex address (0 to 7).

When a receiver or alert unit detects a reportable event (alarm, test, tamper, loss of AC power, and so on) it goes into an “off normal” state. To quickly locate any devices which might be in the “off normal” state, global commands (which are interpreted simultaneously by all of its devices) are issued by the transponder approximately ten times per second. These global commands are followed by commands to specific devices to determine the nature of the “off normal” condition and, in the case of an alarm or test, to obtain the **Transmitter Identification Number**, **Transmitter Battery Condition**, and **Received Signal Strength**. This information is used by the Central Console to identify the subscriber transmitting the alarm (test) and determine the subscriber’s location.

2.2.5 Central Console

The Central Console consists of one to eight IBM PC compatible computers running the Security Escort software within the Microsoft Windows® environment. One computer serves as the main controller for the entire Security Escort System (the master computer) and a second serves as an optional backup (the slave computer). The other computers serve as workstations for the operators of the software. The slave and workstation computers can be used for administrative functions such as adding subscribers or performing routine system tests without interfering with the operation of the master computer.

In the event of an alarm from a transmitter, the console displays the name of the individual to whom the transmitter is assigned, and the location from where the transmission was made. The location information is shown graphically on a map of the protected area. Other information about the subscriber, such as address, home address, phone number, and any disabilities may also be shown.

Both the main computer and the backup record all messages sent between the Central Console and the transponders, providing redundancy of records.

2.2.6 Software overview

The Central Console contains all operating software and databases required by the Security Escort System. The Security Escort *Operation Manual* describes that portion of the system software, which affects system operators (in most cases, the Security Department personnel). This *Technical Reference Manual* discusses only the software functions that are specific to installation and maintenance of the system.

All operations on the Central Console computers are password access controlled. The **Logout** option on the main menu bar produces a screen for entry of the password.

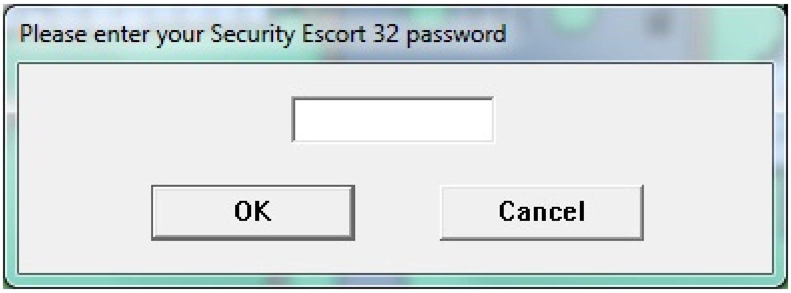


Figure 2.1: Screen for Password Entry

Passwords may have different authority levels, as assigned by installation company personnel or the Security Department's key operator. Operations that are inaccessible at a given authority level appear in gray rather than black on the Central Console. The installation and maintenance portion of the Security Escort Software is designed to facilitate the set-up and modification of the system and to provide rapid diagnosis of system problems, usually with only one person being required. From the Central Console, simple commands can be used to scan all devices on a particular transponder for their current status. Devices can be enabled or disabled from the Central Console and the on-board transmitter of one receiver can be activated to test an adjacent receiver in order to confirm that its radio receiver section is operating properly (buddy check).

The Security Escort software also continually monitors the status of each transponder to insure it is functioning correctly. All communications between the Central Console and a transponder require acknowledgments to verify message integrity. Each transponder must transmit a message periodically, to assure the Central Console that the transponder is still operating properly. Should a transponder fail to transmit either a routine status report or any other message to the Central Console, the Central Console sends a query to the transponder requesting a message be returned. If there is no response after six attempts at communications, a pop-up alert appears on the Central Console.

2.3 System operation

The following sections describe the basic operation of the Security Escort System during alarm, test, and various other routine and emergency situations.

2.3.1 Alarm sequence

Transmitter

When a user of the Security Escort System activates an alarm with the transmitter, multiple identical packets of digital data are transmitted from the hand-held transmitter to nearby receivers. Each packet contains a unique device identification code, an alarm type indication, the transmitter battery condition, and a check sequence. Multiple packets are employed to assure successful receipt of the message by the receivers.

Receiver

The receiver is continuously listening for radio signals that might be alarm or test data from transmitters. If the incoming message is determined to be valid, representing either an alarm or a test from a transmitter, the peak amplitude of the received signal is recorded.

Transponder scanning

The transponder continually scans all of its receivers to see if any of them received a valid transmission. Once a transponder determines that one or more of its receivers received a transmission, it directs a message to those receivers, to determine the specifics of the transmission.

Receiver response

The receivers respond to these messages with the identification code of the transmitter that sent the alarm or test, the alarm or test type, and the amplitude of the signal received from the transmitter.

Transponder data collection and response

The transponder next constructs a message for the Central Console containing the receiver addresses, for all receivers responding to the event and signal levels of the receptions, the alarm or test type and the transmitter identification number. The transponder then verifies that the communications channel is free and transmits the information to the Central Console. If the communication channel is busy, the transponder delays a random period of time and tries again.

Central Console response

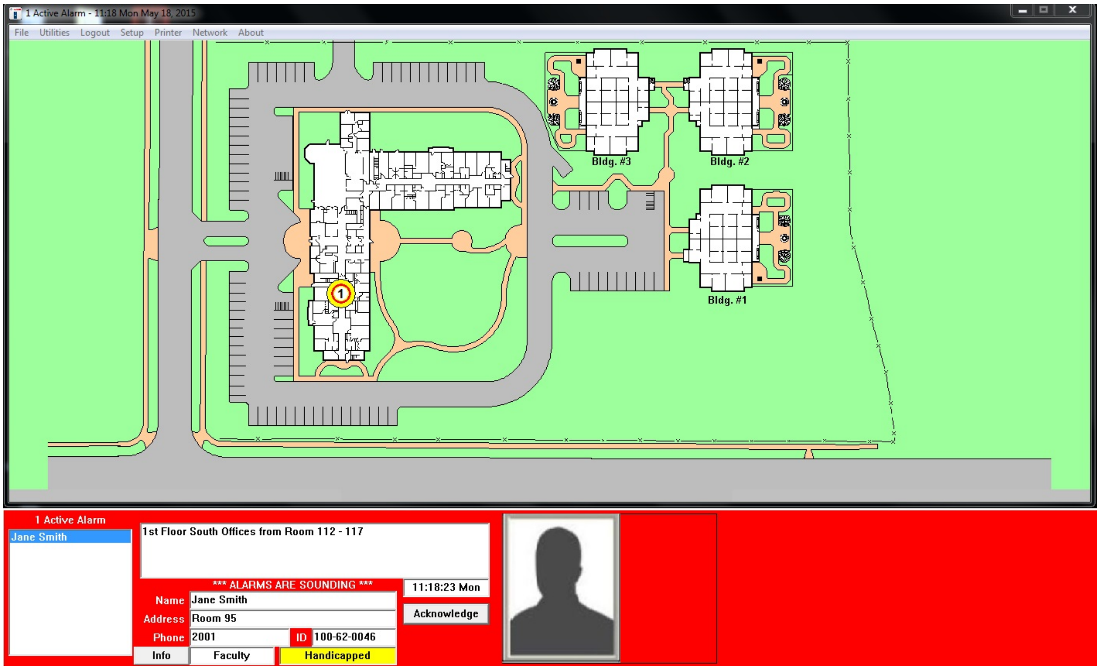
After acknowledging the alarm transmission from the first transponder, the Central Console begins its alarm analysis while collecting the alarm data from all other transponders, which had receivers that detected the alarm. The **Subscriber Database** is checked to determine the appropriate reaction to the alarm. If the transmitter is assigned to a valid subscriber and it is not designated as a security or watchman device, the Central Console commands the transponders to turn on the appropriate alert units. Depending on the settings selected in the **Security Preferences** dialog, this enables only the strobe portion of the alert unit, or both the strobe and siren. If the transmitter is unassigned, or has been disabled by selection of that option in the **Subscriber Database**, no commands will be issued to activate the alert units.

Notice!

An option in the **Security Preferences** dialog allows unauthorized transmitters (not programmed in the database) to be treated like authorized transmitters. For example, strobes and/or sirens can be activated in the case of an alarm transmission (if they are also set to be activated for authorized transmitters).

The Central Console computes the location of the transmitter by comparing the signal strengths measured by the receivers which detected the transmission.

A partial map of the protected area is displayed on the Central Console, centered on the computed location, and, a yellow circle is drawn to assist the operator in guiding the response personnel to the probable source of the transmission. Other data drawn from the **Subscriber Database** is added to the Central Console display to assist in the response to the alarm. In addition, the Central Console enunciator is activated to alert the operator to the event.



1 Active Alarm - 11:18 Mon May 18, 2015

1 Active Alarm

Jane Smith

1st Floor South Offices from Room 112 - 117

*** ALARMS ARE SOUNDING ***

11:18:23 Mon

Name: Jane Smith

Address: Room 95

Phone: 2001

ID: 100-62-0046

Faculty

Handicapped

Figure 2.2: Central Console Screen During Alarm

The Central Console also writes the time, location, and identity information to the hardcopy printer and writes a complete record of all activities to the hard disks on both the primary and backup computers.

Operator response

The operator reacts to the alarm by acknowledging the event with a keystroke or click of the mouse, which silences the alert sound from the Central Console. This silences only the Central Console enunciator, not the outdoor sirens or interior horns. The operator then directs response personnel to the scene and awaits their indication that the problem was resolved.
When the response personnel advise the operator that the problem is under control, the operator enters his password into a box on the Central Console. This step causes the Central Console to send commands to the transponders to silence the sirens and horns and extinguish the strobes and LED's. A reset of the system is accomplished with another key stroke or a mouse click on the **Reset** button on the screen.

Multiple alarms

Receivers can handle multiple separate alarm or test events at the same time. If the receiver's event buffer is full but contains test events, it discards the test records in favor of an incoming alarm. Similarly, the transponder event buffer can hold multiple events and it also replaces test events with alarm events when its buffer is full.
To assure that simultaneous alarms are detected, the multiple identical packets sent by the transmitters are randomly spaced over approximately one second. Only one of the packets must be detected to produce an alarm. Thus a collision between the transmissions of two or more transmitters is virtually eliminated. In addition, unless the transmitters are in the same location, they detect different groups of receivers. The Central Console is capable of

processing 30 concurrent alarms. When there is more than one active alarm, the Central Console displays data for the first to be received and also indicates the total number received and the identity of the individuals transmitting them. The operator can click on the name of an individual to see the data for a particular alarm.

2.3.2 Test sequence

Transmitter

When the user of the Security Escort System activates a test transmission, multiple identical packets of digital data are transmitted. In this case, the digital data in the transmitted packets contain a test code rather than an alarm code.

Receiver

The receiver responds to a test transmission the same as to an alarm transmission by decoding the radio signals, and measuring signal levels.

Transponder data collection and response

The transponder collects data on a test event in the same manner as for an alarm event, it does not command the LED (green for test confirmation) to flash until it has been commanded to do so by the Central Console. Transmitters that are disabled in the **Subscriber Database**, or not in the database at all, do not receive a flashing green light or flashing strobe that would indicate a successful test.

Central Console Response

The Central Console responds to the report of a test from a transmitter by collecting the data from each transponder reporting the event, and recording the locations of the receivers that detected the transmission. In this case, however, it does not calculate a location estimate. It simply records the data on the primary and backup computers’ hard disks, prints the identity of the subscriber, date and time on the hardcopy printout, and displays generic test icons on the Central Console in positions corresponding to the locations of receivers hearing the transmission.

In the case of test transmissions from security transmitters or watchman transmitters, the Central Console determines the closest receiver to the transmission and creates a guard tour event which becomes a part of the **Guard Tour Report**.

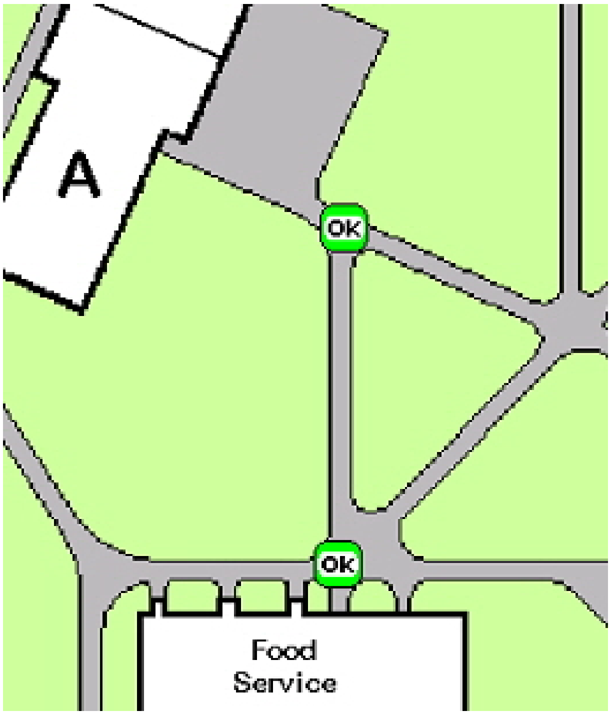


Figure 2.3: Console Screen Showing test Icons

Operator response

There is no response required of the operator in the case of a test transmission.

3 Setting up the system

3.1 Initial system configuration

The default password is PPP. The default password, the master password, and passwords for all system operators should be changed.

- To generate the map file for the screen display, refer to *Map file generation and scaling, page 112*.
- To setup the transponder COMM ports refer to *Transponder comm port setup dialog, page 89*.
- To setup the system COMM ports refer to *Remote comm port setup dialog, page 90*.
- To set the function of the system COMM ports and setup remote access, see *Remote setup dialog, page 92*.
- To program the system configuration, see Transponder Database.
- To program the system responses to an alarm, see *Security Preferences dialog, page 40*.
- To program the system responses to troubles, see *Popup trouble filter dialog, page 60*.
- After communications to the transponders are established for any transponder that uses a Proxim Radio to communicate, program the **Uses Proxim Radio** field in the **Transponder parameter change** dialog. If all alarms are to be silent, program the **Run Silent** field (see *Transponder parameter change dialog, page 72*).
- If this system has master and slave computers, set the Default Master Computer and Default Slave Computer (see *Remote setup dialog, page 92*).
- If using pager access in this system, see *Pager setup dialog, page 97*.
- If this computer runs other programs at the same time, Security Escort is running, set the **Not Always Top Window** field (see *Security Preferences dialog, page 40*).
- To program the ID receiver to automatically enter the transmitter IDs, see *Security Preferences dialog, page 40*.
- To set the names of the subscriber classes, see **System Default** dialog in the Security Escort *Operation Manual*.
- To program the transmitters into the **Subscriber Database**, refer to the Security Escort *Operation Manual*.

4 System menus and screens

4.1 File menu

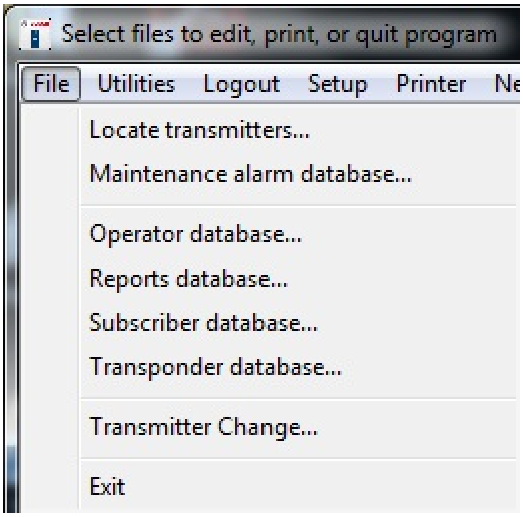
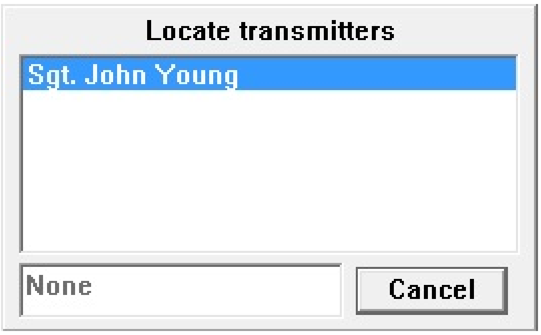


Figure 4.1: File Menu

4.1.1 Locate transmitters

This selection allows the operator to display the last reported location of the transmitter assigned to the indicated individual or asset. When the individual or asset is selected from the list, the time of the last supervision report is shown (or “None” is displayed if no supervision report was received from that transmitter). On the map, the last report location is shown.



Sgt. John Young

None

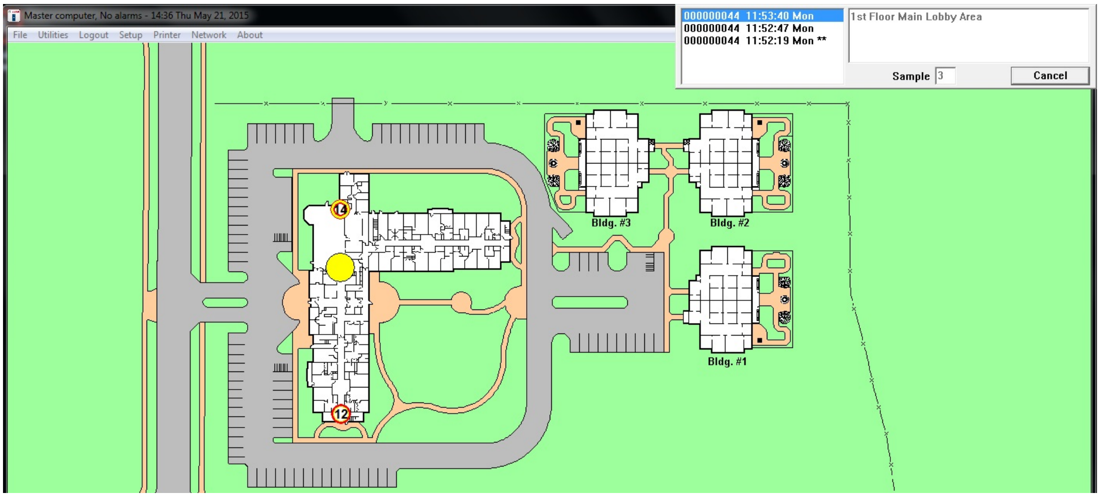
Figure 4.2: Locate Transmitters

4.1.2 Maintenance alarm database

Maintenance transmitters, when activated in the “Test” or “Alarm” mode, generate a series of multiple data packets like subscriber transmitters. However, a special code in each packet identifies the transmitter as a “Maintenance Transmitter”.

The receiver responds to a maintenance “Alarm” or “Test” transmission in the same way it responds to a subscriber “Alarm” or “Test”, unless the receiver has been put in the “Setup” mode. The transponder then reports the maintenance transmitter identification number and all signal levels to the Central Console, which then creates the location estimate and processes the data as it would for a normal alarm.

Notice!
All maintenance transmitters are assumed to be valid so there is no need for the Central Console to check for the identification number in the Subscriber Database.


Master computer, No alarms - 14:36 Thu May 21, 2015

```
000000044  11:53:40 Mon
000000044  11:52:47 Mon
000000044  11:52:19 Mon **
```

1st Floor Main Lobby Area

Sample: 3

Figure 4.3: Maintenance "Alarm” With Signal Levels Shown in Icons

"The Central Console will not generate an audible alert for the operator, nor will it create an “alarm” display on the main Central Console screen. Because they can be set to graphically display received signal levels, maintenance “alarms” are very useful to verify that the system coverage exists at any location in the protected area, and that receiver redundancy is adequate.

4.1.3 Operator Database

The **Operator Database** contains the information on the individuals who are authorized to operate the system, their authority levels, and passwords. See the Security Escort *Operation Manual*.

4.1.4 Reports Database

The **Reports Database** contains information of alarms that were previously processed by the system. Alarm data and maps showing the operators view can be recalled. See the Security Escort *Operation Manual*.

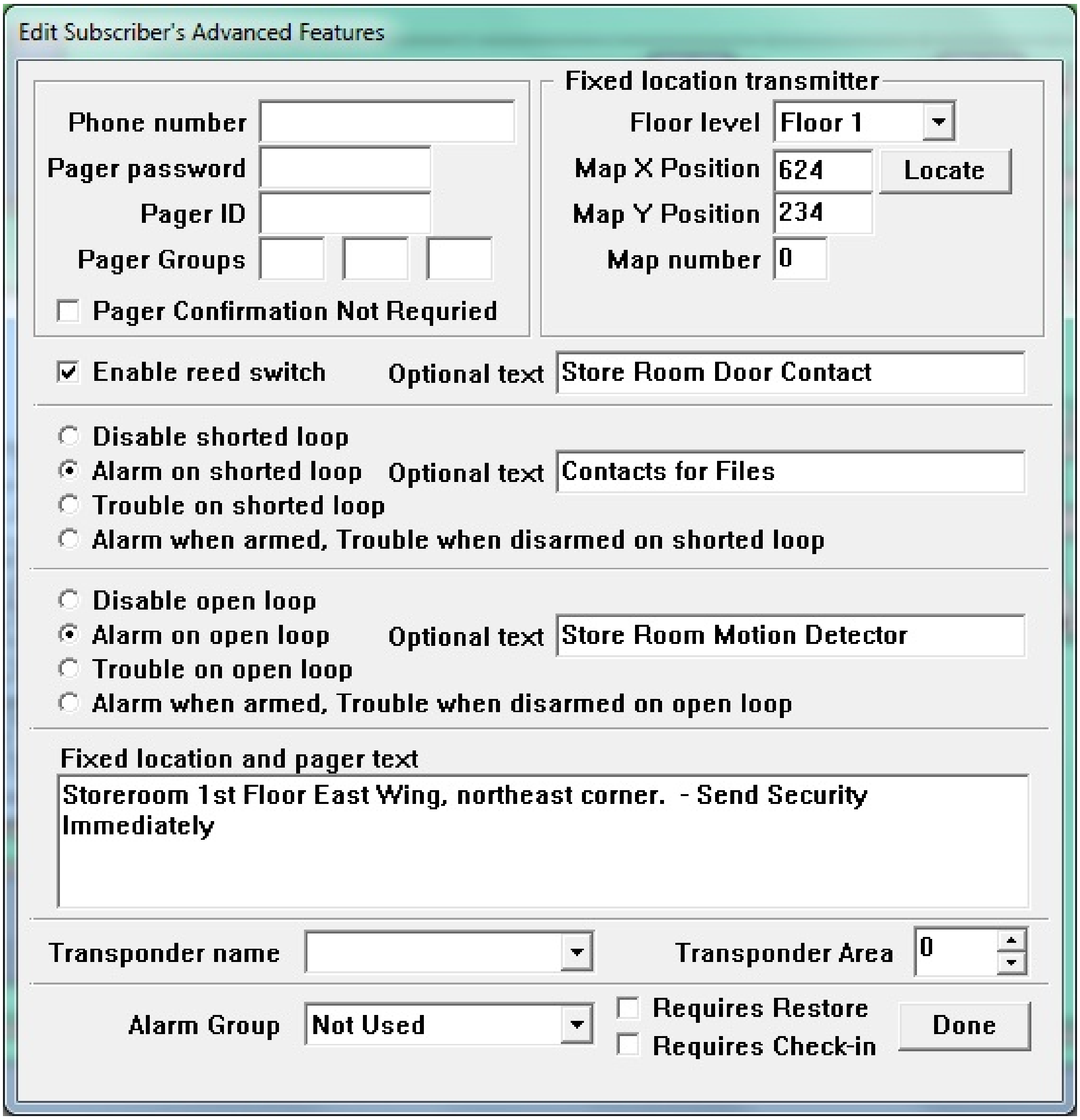
4.1.5 Subscriber Database

The **Subscriber Database** contains the information on the transmitters that are assigned in the system. See the Security Escort *Operation Manual* for the basic operations of the **Subscriber Database** dialog. See the section on Exporting, importing and merging the Subscriber Database for information on the data merge, import and export functions of the **Subscriber Database**.

The following section explains the advanced features of the **Subscriber Database** dialog when you are inserting a new or editing an existing subscriber.

Subscriber’s Advanced Features dialog

Clicking the **[Advanced]** button in the **Edit Subscriber Database** dialog opens the **Edit Subscriber’s Advanced Features** dialog window.



Edit Subscriber's Advanced Features

Phone number
Pager password
Pager ID
Pager Groups
□ Pager Confirmation Not Requried

Fixed location transmitter
Floor level: Floor 1
Map X Position: 624 Locate
Map Y Position: 234
Map number: 0

☑ Enable reed switch Optional text: Store Room Door Contact

○ Disable shorted loop
● Alarm on shorted loop Optional text: Contacts for Files
○ Trouble on shorted loop
○ Alarm when armed, Trouble when disarmed on shorted loop

○ Disable open loop
● Alarm on open loop Optional text: Store Room Motion Detector
○ Trouble on open loop
○ Alarm when armed, Trouble when disarmed on open loop

Fixed location and pager text
Storeroom 1st Floor East Wing, northeast corner. - Send Security Immediately

Transponder name Transponder Area: 0

Alarm Group: Not Used
□ Requires Restore
□ Requires Check-in
Done

Figure 4.4: Subscriber's Advanced Features Dialog

The **Edit Subscriber's Advanced Features** dialog is used to set up special transmitters that monitor fixed locations, subscriber pager access, parameters for point transmitters, the virtual fence for a wandering alarm, the alarm group for arming of the transmitter and check-in requirements for this transmitter.

Phone number This phone number is dialed to send a pager message to this subscriber. Typically, this is a different phone number than the one that is manually dialed to access this pager. The phone number is assigned by the paging service.

Pager password This is the password to be sent to the paging service when a page is sent to this subscriber. Leave blank if not required (typically the pager password is not required). The pager password is assigned by the paging service.

Pager ID
This is the ID that identifies the pager to receive the pager message (many times this value is the last 7 digits that would be manually dialed to access this pager). The pager ID is assigned by the paging service.

Pager Groups
These are the pager groups that this subscriber is a member of. This subscriber may be a member of up to 3 different pager groups.

Pager Confirmation Not Required
If checked, the confirmation pager message is not sent to this pager if alarm is acknowledged by an acknowledgement transmitter.

Fixed location transmitter
This section is to be used only when this transmitter is mounted in a fixed location (it does not move). When this transmitter transmits and alarm it will always be reported at the programmed location.

Floor level
This is the floor level where this alarm is to be located for a fixed location transmitter.

Map X Position
This is the X coordinate of the map position where this alarm is to be located for a fixed location transmitter.

Map Y Position
This is the Y coordinate of the map position where this alarm is to be located for a fixed location transmitter.

Locate
When clicked, the dialog will disappear and the cursor will change to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button will scroll the map so that point is at the center of the screen.

When the map is showing the desired alarm location, move the cross hair to the exact location of the alarm to be reported and click the right mouse button. The dialog will reappear and the selected location will be entered into the X and Y coordinates.

If while the cross hair cursor is being displayed, you desire to exit without changing any coordinate values, press the <Esc> key and the transponder edit dialog will reappear.

Map number
Defines which bitmap is to be displayed for the fixed location of this transmitter. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the “Escort” sub-directory. Map 1 would be MAP1.EDB. There can be 100 maps per Security Escort system (0-99).

Enable reed switch
If checked the reed switch input of this transmitter enabled to cause an alarm. Otherwise the reed switch input will be disabled. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Optional text
This is optional text that will be added to the location text when this input reports an alarm. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Disable on shorted loop
If selected, a shorted loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Alarm on shorted loop If selected and the alarm group, where this transmitter is assigned to, is armed, then a shorted loop on this transmitter will cause an alarm report to be displayed. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Trouble on shorted loop If selected, a shorted loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Alarm when armed, Trouble when disarmed on shorted loop If selected and the alarm group, where this transmitter is assigned to, is armed; then a shorted loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then a shorted loop on this transmitter will cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Disable open loop If selected, an open loop on this transmitter will not cause an alarm or trouble report to be displayed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Alarm on open loop If selected and the alarm group, where this transmitter is assigned to, is armed, then an open loop on this transmitter will cause an alarm report to be displayed. The alarm group, where this transmitter is assigned to, must be armed for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Trouble on open loop If selected, an open loop on this transmitter will cause a trouble report to be displayed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Alarm when armed, Trouble when disarmed on open loop If selected and the alarm group, where this transmitter is assigned to, is armed; then an open loop on this transmitter will cause an alarm report to be displayed. If selected and the alarm group, where this transmitter is assigned to, is disarmed, then an open loop on this transmitter will cause a trouble report to be displayed. If no alarm group is assigned, the transmitter is always armed. For this option to be enabled, the transmitter’s class must be set to “Point type”.

Fixed location and pager text This is the text that will be displayed as the location of the alarm for fixed location transmitters and on pagers reporting this alarm.

Transponder name Select the transponder with the area that is defined for a wandering (virtual fence) alarm. See **Transponder Area** below for the operation and setup of the wandering alarm (virtual fence alarm).

Transponder Area

Wandering alarm - Create a protected area by placing a virtual monitor “fence” around an area of the main map. These areas are defined in the **Transponder Database**. If this transmitter is constrained to remain within one of these defined areas, first select the defining transponder in **Transponder name** above. Then select the desired area from this drop-down list of the transponder’s area names.

For the wandering alarm to work, the supervision period must also be programmed for this transmitter.

Then specific transmitters are marked in the subscriber database, to be constrained within a specific fenced area defined by this option. If the transmitters leave their defined area, the system will report this as a Wandering alarm and continue to monitor and track the location of the transmitter until the alarm is canceled from the screen in the normal way. However, these tracking updates can only occur every supervision transmission period (not on an accelerated rate like a tracking alarm).

The Security Escort system computes the location of the transmitters when they broadcast automatic supervision transmissions periodically.

Because of the basic location accuracy and the floor-to-floor accuracy of the system, there is a potential for some false alarms. If false alarms are a problem, check the **Filter Virtual Fence** checkbox in the **Security Preferences** dialog. If you do this, two successive location calculations will have to indicate the transmitter has moved outside the protected area before an alarm is generated. The downside of this is a delay in the reporting of a wandering alarm of one extra transmitter supervision period.

Alarm Group

This is the alarm group that controls the arm/disarm status of this transmitter. Select the desired alarm group from the dropdown list of the alarm group names. This alarm group must be armed, for this transmitter to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed.

Requires Restore

When this checkbox is checked, transmitter will have to be restored.

Requires Check-in

When this checkbox is checked, this transmitter will have to be activated once each day during the **Check-in Schedule** time. At the end of the check-in period, if the subscriber fails to check-in, a **Failed to Check-in Report** will be generated and presented to the operator of the software. This report contains all of the people who failed to check-in with their first address line and phone number. All subscribers in the report must be checked on to make sure they are not in need of assistance, as this may be a life-treating situation. A printed report may also be generated.

If the transmitter is not a point type, then the transmitter can generate alarms and therefore a test transmission will be used for the check-in.

If the transmitter is a point type, then any non-trouble transmission will serve as a check-in.

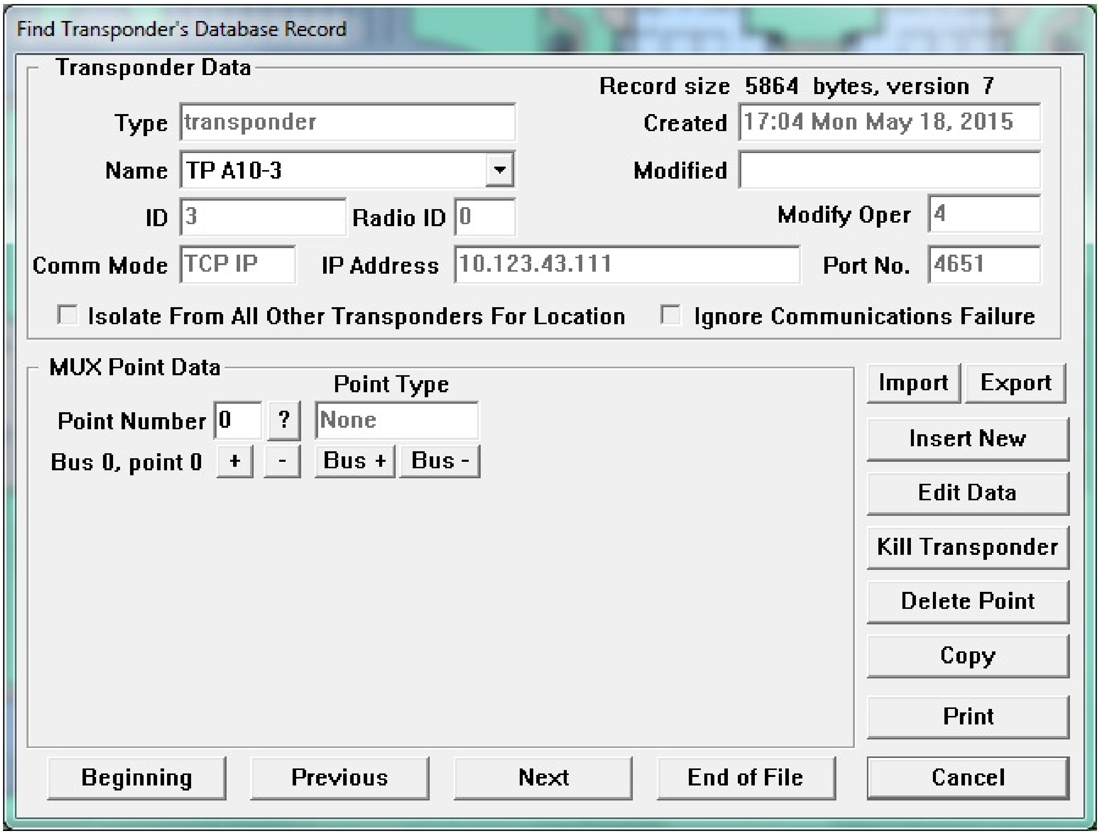
One of the 10 schedules must be selected as the check-in schedule to define the check-in period.

Done

Click this button when all changes to this dialog are completed and return the main **Subscriber Database** edit dialog.

4.1.6 Transponder Database

The **Transponder Database** is established at system set-up and contains all necessary configuration data for each transponder, receiver and alert unit. It describes the basic structure of the installation, including all device names, locations, types, multiplex addresses, etc. This information is used by the Central Console to generate alarm and test displays on the Central Console and in determining which alert units are to be activated.



Find Transponder's Database Record

Transponder Data

Record size 5864 bytes, version 7

Type: transponder

Created: 17:04 Mon May 18, 2015

Name: TP A10-3

Modified:

ID: 3

Radio ID: 0

Modify Oper: 4

Comm Mode: TCP IP

IP Address: 10.123.43.111

Port No.: 4651

☐ Isolate From All Other Transponders For Location

☐ Ignore Communications Failure

MUX Point Data

Point Number: 0

Point Type: None

Bus 0, point 0

Figure 4.5: Find Transponder's Database Dialog

Access the **Transponder Database** from the **File** menu on the main menu bar. The following table describes the elements of the **Find Transponder's Database Record** dialog.

Type
This field indicates the type of transponder record that you are currently viewing. Currently, there is only one type of transponder available.

Name
This drop-down list contains the names of the transponders. Selecting the name of the transponder in the drop-down list displays information of the transponder record in the dialog window. The transponder names are assigned during set-up and are used to indicate the physical location of the transponder, or the region of the protected area covered by a particular transponder.

Created
Modified
Modify Oper
The system software automatically creates these 3 fields to the right of the **Find Transponder's Database Record** dialog. They represent the date the transponder was first entered into the **Transponder Database**, the date of the last change of any entry for this transponder, and the identity of the operator making the last change (determined from the password entered to make the change).

ID
This is a number assigned to the transponder at system set-up. It is used by the Central Console to identify the transponder during all communications between the Central Console and the transponder. The number must agree with the transponder address, which is set during final installation using switches on the transponder circuit board.
Note: The number 0 is not allowed as a transponder address.

Radio ID
This is the identification number for the radio interface unit, if the transponder communicates to the Central Console by means of a radio link. (This feature is currently not implemented)

Comm Mode
This indicates which communication mode that the Central Console is using to communicate with the transponder.

IP Address
If the **Comm Mode** is “TCP IP”, this field will appear in the dialog window. This field indicates the IP address assigned to the transponder.

Port No.
If the **Comm Mode** is “TCP IP”, this field will appear in the dialog window. This field indicates which Central Console communications port will be used to communicate with this transponder.

Comm Port Index
If the **Comm Mode** is “RS232”, this field will appear in the dialog window. This field indicates which Central Console communications port will be used to communicate with this transponder. The **Transponder Comm Port Setup** dialog selects the specific physical port that this index will refer to.

Isolate From All Other Transponders For Location
When checked, this transponder is isolated from all other transponders for location considerations. This should be used when distant transponders sometimes hear an alarm and throw off the alarm location calculation. If this checkbox is checked, it indicates that this transponder is protecting an area that is independent of all other transponders in the system. When an alarm is reported, and receivers on this transponder have the best reception, only the receivers on this transponder will be considered for the location of this alarm. If another transponder has the best reception, then the receivers on this transponder will be ignored for the location of this alarm.

Ignore Communications Failure
This checkbox allows communications failures to be ignored for this transponder. It is used during a new installation for transponders that are not yet fully on line. During system maintenance, when a transponder is out of service for a while, it is used so that the communications failure messages will not flash on the screen and distract the operator. **Checking this checkbox causes the system to ignore communication failure. Therefore, if communications fail with this transponder, the area this transponder protects will not be protected, and alarms from subscribers in that area will be missed without the operator's knowledge. This checkbox should not be checked in a live system.**

[Insert New]
Clicking this button displays a new **Edit Transponder's Database Record** dialog window. This is used to enter a new transponder to the database.

[Edit Data]
Clicking this button allows the currently displayed transponder's database record to be modified.

[Kill Transponder]
Clicking this button deletes the currently displayed transponder's database record. If the transponder is "killed", its data is permanently deleted and cannot be recovered.

[Delete Point]
Clicking this button deletes the currently displayed point from the current transponder's database record. If the point is deleted, its data is permanently deleted and cannot be recovered.

[Copy]
Clicking this button copies the currently displayed transponder's database record into a new transponder record. This allows similarly configured transponders to be programmed once then copied into a new record.

Note: It is not possible to edit the Transponder ID itself. If this should be necessary, the [Copy] button can be used to produce another Transponder Database entry duplicating the first, but with the Transponder ID blank. The new Transponder ID can be entered, the new data saved by using the [Save] button, and the old transponder entry can be deleted using the [Kill Transponder] button.

[Print]
Clicking this button prints the currently displayed transponder's database record.

[Beginning]
Clicking this button changes the currently displayed transponder to the first transponder in the database.

[Previous] Clicking this button changes the currently displayed transponder to the previous transponder in the database.

[Next] Clicking this button changes the currently displayed transponder to the next transponder in the database.

[End of File] Clicking this button changes the currently displayed transponder to the last transponder in the database.

MUX Point Data

The lower section of the **Find Transponder's Database Record** dialog window provides information on the devices controlled by the selected transponder record.

Two digits represent each receiver or alert unit address. The first is the number of the multiplex bus on which the device is mounted (0 to 7) and the second is the multiplex point address assigned to the particular device. On each of the eight multiplex busses, up to 8 devices may be installed, but each device must be assigned a unique multiplex point address (0 to 7). More than one device can have a particular multiplex point address, but only on different busses. The multiplex point addresses are assigned by switch settings on the device (receiver or alert unit) circuit boards. These multiplex point address settings are also a part of the **Transponder Database**. The multiplex address shown in the **Transponder Database** and the multiplex address set on the device circuit board must agree. The **Transponder Setup** dialog is used to verify multiplex address settings.

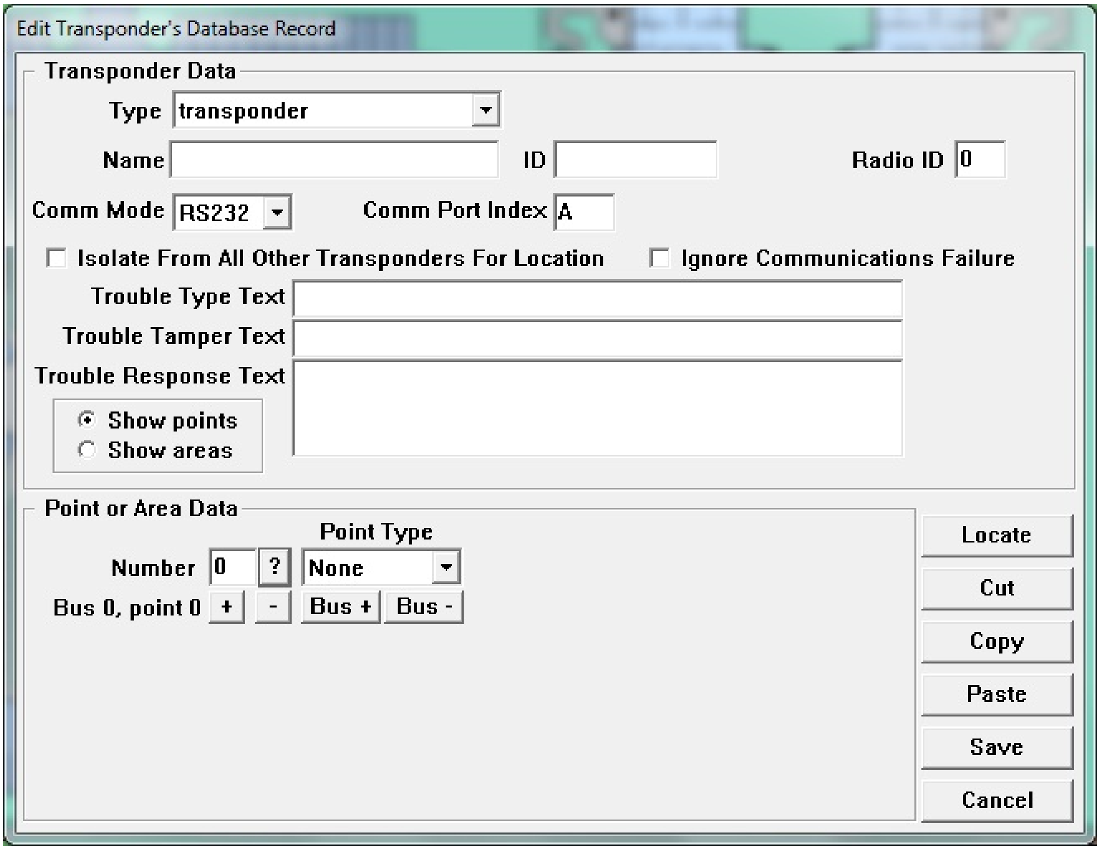
Notice!

It is a good idea to create an entry in the **Transponder Database** for each transponder in the system before entering the data for each device, so that all transponders appear in the drop-down menus.

Creating a new transponder entry

Creating and modifying the **Transponder Database** requires special authority levels usually assigned only to the installing company's personnel. Clicking the **[Insert New]** button opens a new **Transponder Database** dialog window.

The **System Design Layout Sheets** prepared in advance by the installation manager should contain the necessary information for assigning the **Transponder Name** and **ID**, the **Comm Port** or **Radio ID**, as well as the names and multiplex addresses for all receivers and alert units connected to each transponder. The layout sheets will also contain the text to be used to indicate the receiver locations and will designate the alert units to be driven by each receiver.



Edit Transponder's Database Record

Transponder Data

Type: transponder

Name:

ID:

Radio ID: 0

Comm Mode: RS232

Comm Port Index: A

□ Isolate From All Other Transponders For Location

□ Ignore Communications Failure

Trouble Type Text:

Trouble Tamper Text:

Trouble Response Text:

● Show points

○ Show areas

Point or Area Data

Number: 0

Point Type: None

Bus 0, point 0

Figure 4.6: Blank Dialog Resulting from Selection of [Insert New] Button

The new elements of the **Edit Transponder's Database Record** dialog.

Trouble Type Text This is the text that will be shown in the trouble dialog when the remote key input on the transponder goes active (shorted).

Trouble Tamper Text This is the text that will be shown in the trouble dialog when the remote key input on the transponder goes into trouble (open).

Trouble Response Text This is the text that will be shown in the trouble dialog as the response test. The actions the responding individual should take.

Show Points If selected, the lower section of the **Transponder Database** dialog will show the point's (receiver, virtual receiver or alert unit's) database values.

Show Areas If selected, the lower section of the **Transponder Database** dialog will show the alarm area's database values.

Setting receivers parameters

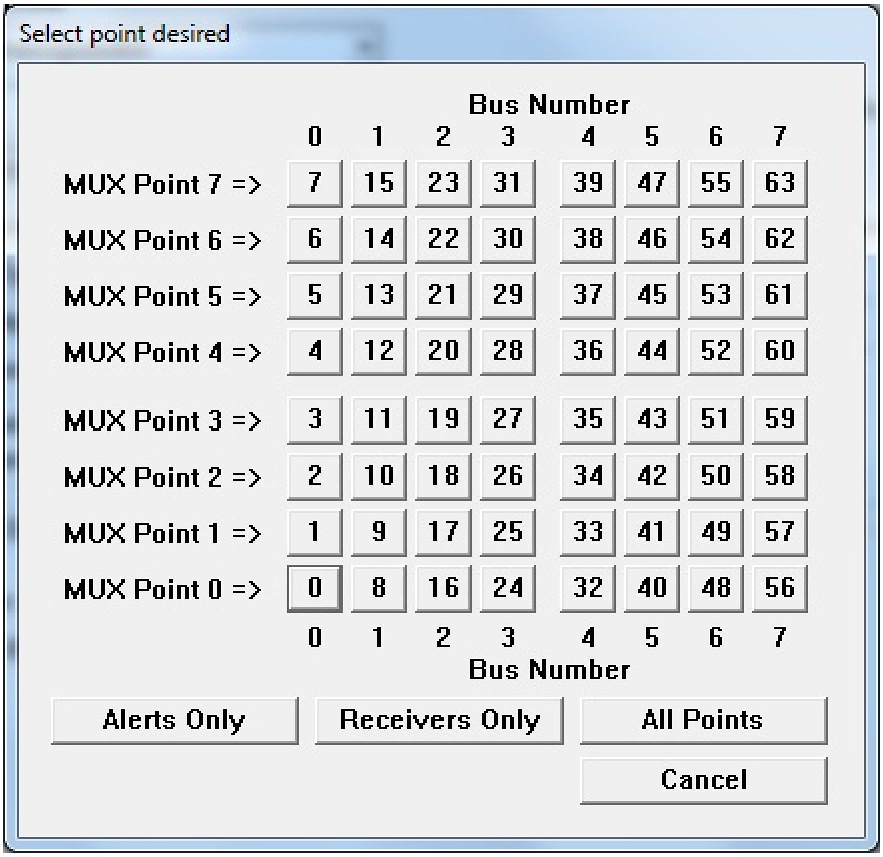
Create or modify the receivers of the transponder using the features of the **Point** or **Area Data.** For configuring **Area Data**, refer to the *Alarm area setup* section. The sections below explain how to configure the receiver points for the transponder.

Entering point number

Each receiver and alert unit connected to the transponder has a unique **Point Number** assigned during the system design process. This **Point Number** ranges from 0 to 63, and corresponds to a specific bus number and point multiplex address number. The multiplex address, set by means of switches on the device (receiver or alert unit) itself, must correspond with the **Point Number** assigned in the **Transponder Database**.

There is a one-to-one relationship between the **Point Number** and the combination of **Multiplex Point Address** / **Bus Number** pair. For example, a device programmed with **Multiplex Point Address** location 3 on **Bus Number** 5 would correspond to the **Point Number** 29.

Clicking the **[?]** button to the right of the **Point Number** text box opens a dialog window displaying the **Point Number** in a table. Clicking on any **Point Number** in the table automatically closes this window and fills the number in the **Point Number** field on the **Transponder Database** dialog. The **Bus number** and **Point address** are also changed to reflect the selection.



Bus Number	0	1	2	3	4	5	6	7
MUX Point 7 =>	7	15	23	31	39	47	55	63
MUX Point 6 =>	6	14	22	30	38	46	54	62
MUX Point 5 =>	5	13	21	29	37	45	53	61
MUX Point 4 =>	4	12	20	28	36	44	52	60
MUX Point 3 =>	3	11	19	27	35	43	51	59
MUX Point 2 =>	2	10	18	26	34	42	50	58
MUX Point 1 =>	1	9	17	25	33	41	49	57
MUX Point 0 =>	0	8	16	24	32	40	48	56

Figure 4.7: Select Point Dialog with "All Points" Selected

This table provides a quick way to select a particular device without having to translate between the two numbering (**Bus Number/Point Address**) systems. The three buttons at the bottom of this dialog allow the user to display:

1. all possible device numbers (**[All Points]** button) regardless that the particular transponder has a device assigned to the number,
2. only locations populated by receivers (**[Receivers Only]** button), or
3. only locations populated by alert units (**[Alerts Only]** button).

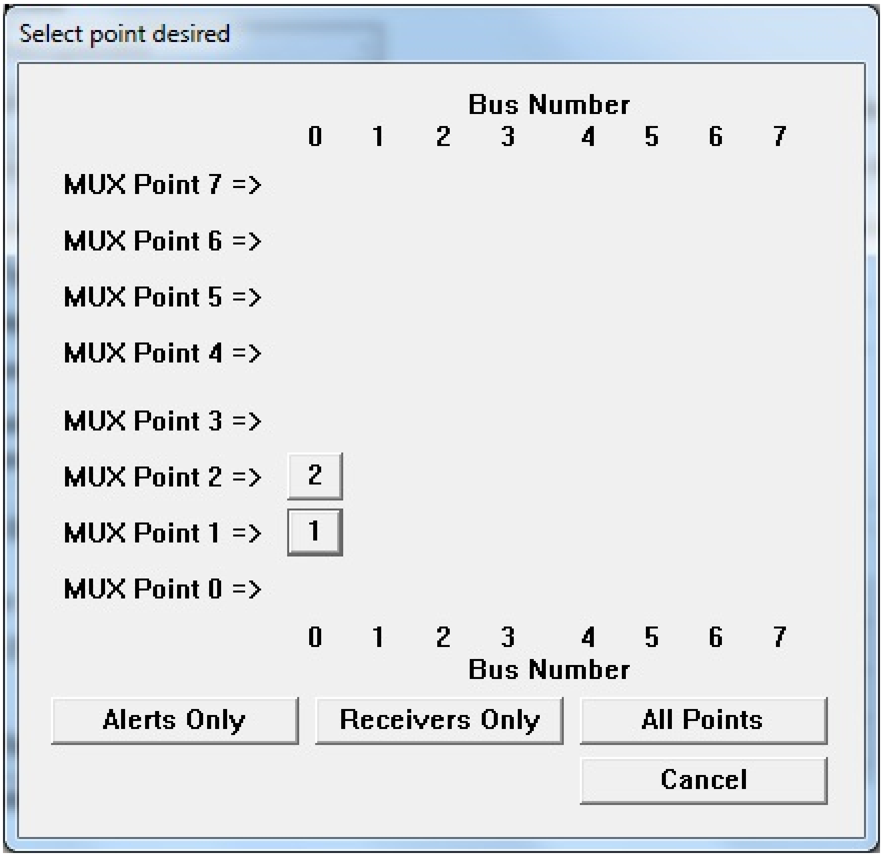


Figure 4.8: Select Point Dialog with "Receivers Only" Selected

Alternatively, the **[+]**, **[-]**, **[Bus +]** and **[Bus** –] buttons, just below the **Point Number** and **Point Type**, allow the user to quickly advance the device selection by one location, either one **Point** location (**[+]** or **[-]**) or one **Bus** number (**[Bus +]** or **[Bus -]**). This is useful when a task requires proceeding from device to device, as during system setup or check out. The **[?]** button is used to display all devices to facilitate quick selection of a particular device. It is most useful when diagnosing a problem with a particular device.

Selecting the Point Type

The **Point Type** drop-down list indicates the type of device at the location currently selected in the **Point Number** field. Once the **Point Number** text box contains the proper value, the device type can be selected from the **Point Type** drop-down list.

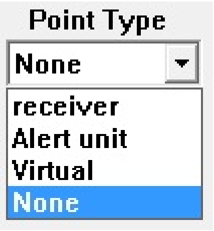
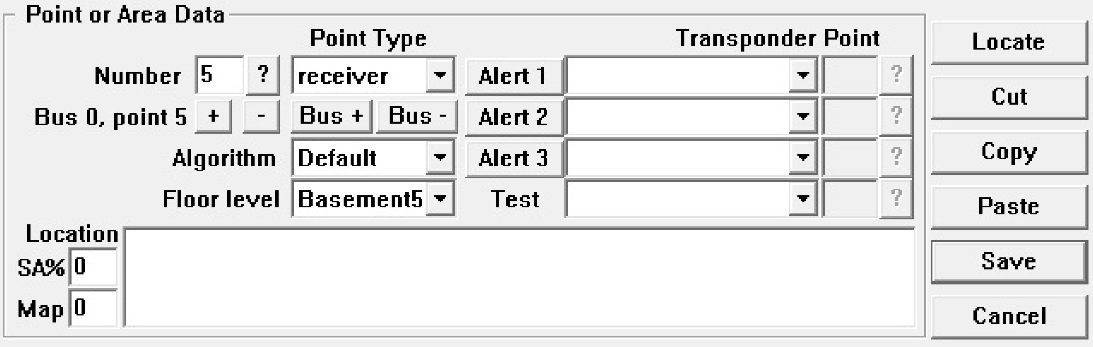


Figure 4.9: Drop-Down List for Selection of Point Type

The valid point types are “receiver”, “Alert unit”, “Virtual” receiver, and “None”. Select the **Point Type** device accordingly when there is a physical device connected at this bus location.

Selecting “receiver” as the Point Type



Point or Area Data

Number: 5

Bus 0, point 5

Point Type: receiver

Algorithm: Default

Floor level: Basement5

SA%: 0

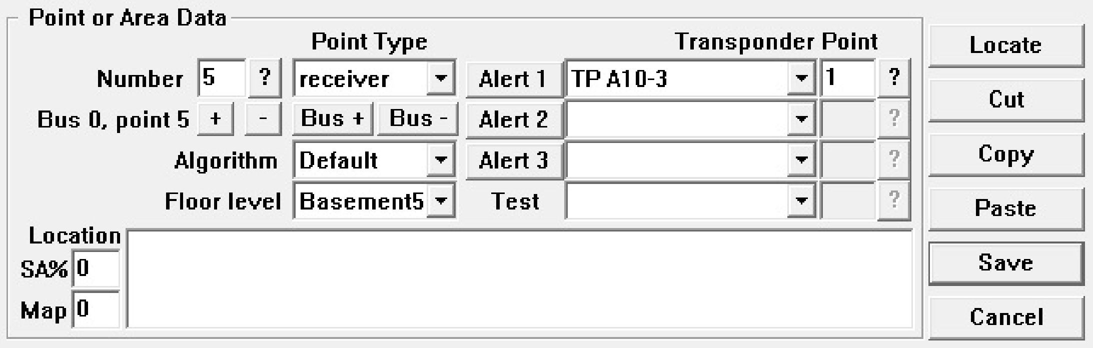
Map: 0

Figure 4.10: Data Entry after Selection of Receiver Point Type

Each receiver can be assigned up to three alert units that are to be activated if it is one of the receivers reported by the transponder as part of an “Alarm” event. Each receiver can also be assigned one alert unit that is to be activated to confirm “Test” transmissions. These alert units need not be connected to the same transponder as the receiver.

To assign alert units to each receiver, the drop-down lists of **Alert 1**, **Alert 2**, and **Alert 3** fields are used to select the transponder of the designated alert unit. The point number can be keyed into the **Point** text box, or click the **[?]** button to display the receiver selection table. Click the receiver number on the selection table dialog to populate the **Point Number** in the **Point** text box.

Similarly, any alert unit, whose strobe unit is to be activated in the event of a “Test” transmission from a transmitter, can be assigned using the drop-down lists of **Test** field.



Point or Area Data

Number: 5

Bus 0, point 5

Point Type: receiver

Algorithm: Default

Floor level: Basement5

Alert 1: TP A10-3, Transponder Point: 1

SA%: 0

Map: 0

Figure 4.11: Assigning Alert Unit to Receiver Point Type

Use the **Floor Level** drop-down list box to assign the physical floor level where a receiver is mounted at.

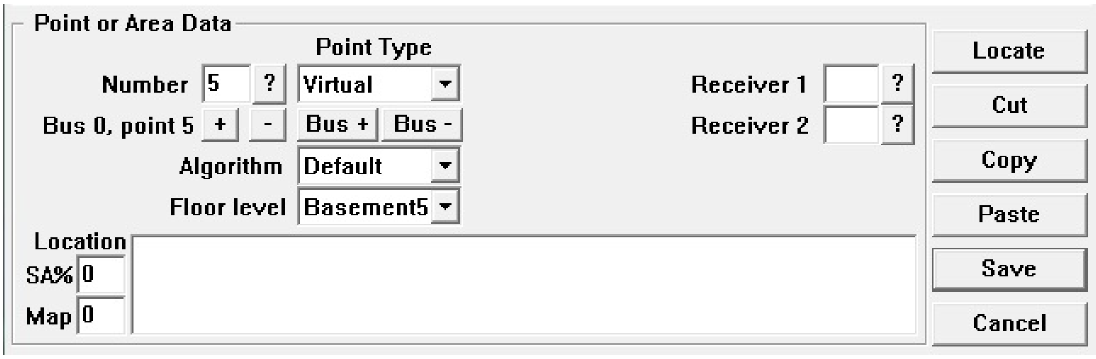
The **Location** field contains the text to be displayed on the Alarm Screen, if this receiver is one of those closest to the alarm source. The description is developed with the guidance of the security personnel who must respond to an alarm. It is vital that the description be clear and unambiguous to them.

To enter a location description, place the cursor in the **Location** field, click the mouse, and begin typing. Receiver and alert unit location names are important because they are used for directing response to an alarm and aid service personnel in identifying the device in the event of a problem. The Problem Reports displayed on the central console and printed by the hardcopy printer contain the device location descriptions that are entered in the **Location** field.

The **Map** field defines which bitmap to display for this receiver or area when an alarm is closest to it. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the Security Escort sub-directory. Map 1 is MAP1.EDB. There can be 100 maps per Security Escort System (0 to 99).

Selecting “Virtual” receiver as the Point Type

Use the “Virtual” selection when there is no physical device connected at this bus location. Starting with version 2.03 of the Security Escort software, you can add “Virtual” receivers in the **Transponder Database**. A “Virtual” receiver is added at one of the 64 points allowed per transponder. However, there is no physical hardware used.



Point or Area Data

Number: 5

Point Type: Virtual

Bus 0, point 5

Algorithm: Default

Floor level: Basement5

Receiver 1:

Receiver 2:

Location

SA%: 0

Map: 0

Figure 4.12: Data Entry after Selection of Virtual Receiver Point Type

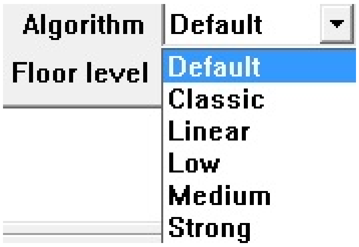
The “Virtual” receiver is intended to compensate in cases where there is a receiver imbalance. For example, if a building with a dense population of receivers is adjacent to a fence with few receivers and an alarm occurs between them; the alarm location may pull towards the building. The “Virtual” receiver references two other physical receivers that must be on the same transponder. Only if both of the referenced receivers receive an alarm transmission, then the “Virtual” receiver will be added to the alarm as if was a physical receiver that heard the alarm at the average receive level of the 2 referenced receivers.

Both the referenced receivers are configured in the **Receiver 1** and **Receiver 2** fields. These are the two receivers, on the same transponder, that a “Virtual” receiver assumes the average of. Both receivers must receive a signal before the “Virtual” receiver reports it also received a signal that is the average of the other two receivers signals. The location algorithm and sensitivity adjust work the same for a “Virtual” receiver as for a physical receiver. Enter the receiver’s **Point Number** in the fields, or click the **[?]** button to select the receiver accordingly. The “Virtual” receiver’s location and sensitivity may be adjusted the same as a physical receiver. After a “Virtual” receiver is added, verify the surrounding areas to make sure they have not been adversely affected. **In no event should a “Virtual” receiver be utilized as a cost savings measure to avoid the installation of an actual receive**r.

For explanations of **Floor level**, **Location** and **Map** fields, please refer to section *Selecting “receiver” as the Point Type***.**

Selecting the algorithm

Starting with version 2.03 of the Security Escort software, there are 5 different location algorithms that can be selected on an individual receiver basis in the **Transponder Database**. “Classic” (original Security Escort algorithm), “Linear”, “Low” pull, “Medium” pull and “Strong” pull. By default when a receiver is set for outside or tunnel, it will use the “Linear” algorithm and all other receivers will use the “Low” pull algorithm. The receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm.



Algorithm Default

Figure 4.13: Location algorithm selection

Changing the algorithm setting for a receiver only affects the location when the alarm is close to this receiver and it hears the alarm the strongest. The stronger the pull the more the alarm will be pulled towards the receiver, with linear having no extra pull.

The algorithm setting will only be available if the **Enable algorithm tweaks** checkbox is checked in the **System Preferences** dialog. Also starting with version 2.03 of the Security Escort software, individual receiver sensitivity can be set in the **Transponder Database**. Receivers can be adjusted from 50% to 149% of their normal sensitivity using the **SA%** setting.

Adjusting the Sensitivity (SA%)

Security Escort software version 2.03 and higher allow individual receiver sensitivity to be set in the **Transponder Database**. Receivers can be adjusted from 50% to 149% of their normal sensitivity. No physical receiver changes or upgrades are required. This setting should only be changed if there are known location accuracy problems in the area of this receiver. Settings of 50 to 99 desensitize the receiver to 50% to 99% of the actual received signal strength. Settings of 1 to 49 increase the sensitivity to 101% to 149% of the actual received signal strength. Try changing the sensitivity of receivers one at a time while testing the alarm location response. For example, if alarms are being pulled towards a particular receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. Generally, it is better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step.

The **SA%** option is only available if the **Enable algorithm tweaks** checkbox is checked in the **System Preferences** dialog. Also in the **Transponder Database**, the **Algorithm** dropdown list allows selection of “Default”, “Classic”, “Linear”, “Low”, “Medium” or “Strong” pull location algorithms for each transmitter. The point reporting the best reception level determines the actual algorithm used for the location on any event. If programmed as “Default”, the algorithm used is “Linear” for points programmed as outdoor or tunnel. All other points use “Low”. If the point reporting the best reception level is not programmed for the “Default” algorithm, the location calculation uses the algorithm programmed.

Other miscellaneous command buttons

The functions of the other miscellaneous command buttons are as of below:

[Locate]

When clicked, the **Edit Transponder's Database Record** dialog disappears and the cursor changes to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button scrolls the map so the point is at the center of the screen and all previously defined receivers and areas are shown with numerical labels.

When the map is showing the location of the desired receiver, move the cross hair to the exact location of the receiver and click the right mouse button. The **Edit Transponder's Database Record** dialog reappears and the selected location is entered into the X and Y coordinates.

When the map shows the desired location, move the cross hair to the exact location of the first point of the polygon that describes the boundary of the area and right click. Move the cursor to the second point of the polygon and again right click. The computer draws a straight line between the first and second points. Repeat this process drawing all sides of the polygon to define the area. To close the polygon, place the last point on top of the first point. The polygon can have up to nineteen sides and no two lines of the polygon may cross each other. If you try to create more than nineteen sides, the computer automatically closes the polygon with the nineteenth side. When the polygon is closed, it can be crosshatched to make it more visible. After the polygon is complete, double click the left mouse button to return to the **Edit Transponder's Database Record** dialog.

If the area being defined is a virtual monitor "fence" area for wandering alarms, the monitor fence (area boundary) should be drawn at least 7.62 m (25 ft) past the area to be protected to reduce potential false alarms. This is due to the basic location accuracy of the Security Escort system.

If the cross hair cursor is displayed and you want to exit without changing any coordinate values, press the <Esc> key and the **Edit Transponder's Database Record** dialog reappears.

[Cut]

Clicking this button copies the displayed point or area data to a clipboard and returns all values to their defaults.

[Copy]

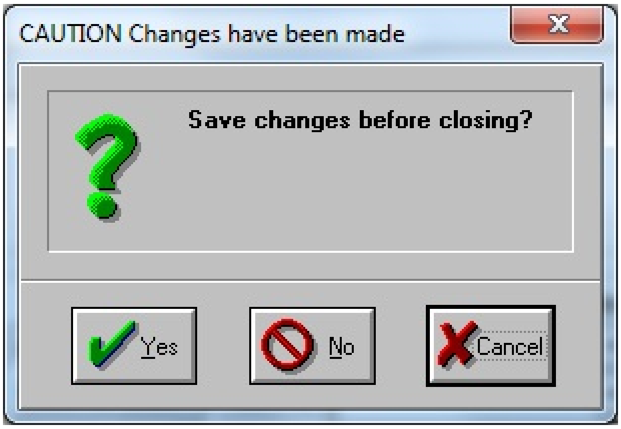
Clicking this button copies the displayed point or area data to a clipboard. Displayed values are not changed.

[Paste]

Clicking this button copies the clipboard values to the displayed point or area data. The values on the clipboard are not changed and can be copied to more points or areas.

[Save] Clicking this button saves all changes to the database.

[Cancel] Clicking this button closes the dialog. If changes were made, the dialog below gives you another chance to save the changes by clicking the **[Yes]** button.

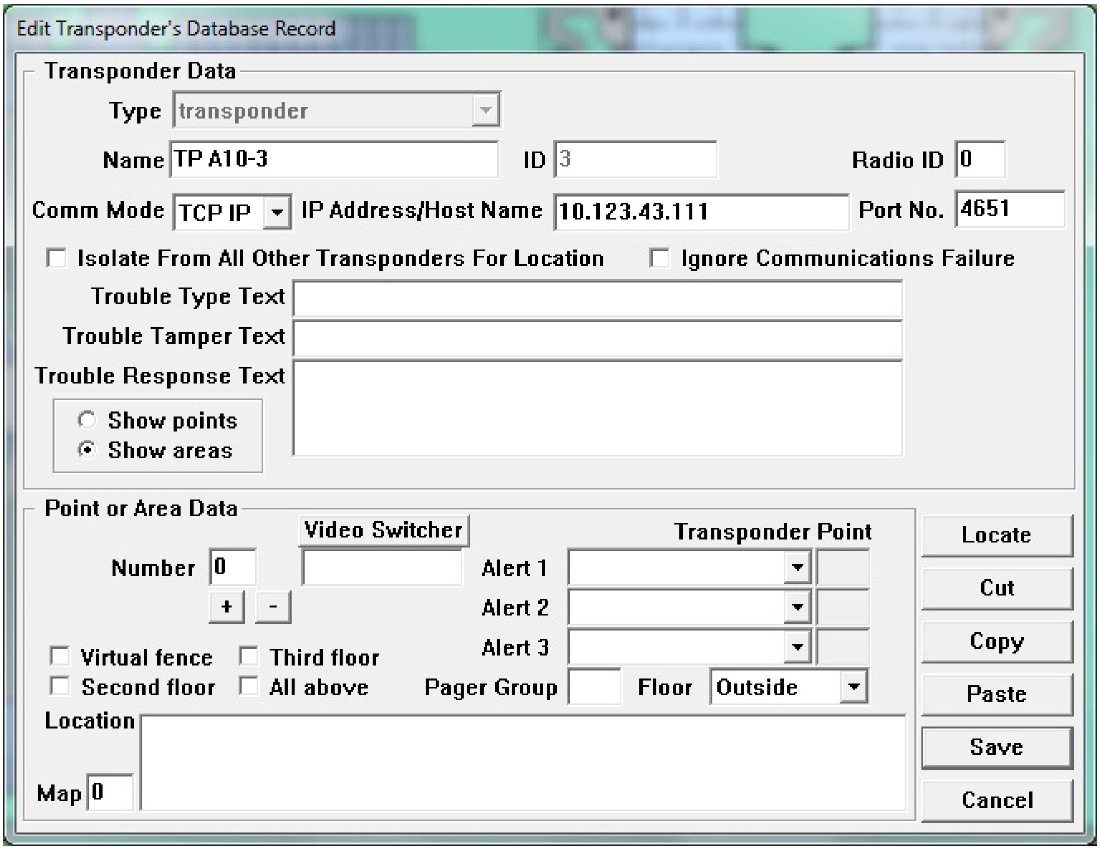


CAUTION Changes have been made

Save changes before closing?

Alarm area setup

In the **Transponder Database** under the **File** menu, select the transponder where the alarm area is to be programmed in. Click the **[Edit Data]** button, followed by **Show areas** radio button and select the desired area.



Edit Transponder's Database Record

Transponder Data

Type: transponder

Name: TP A10-3 ID: 3 Radio ID: 0

Comm Mode: TCP IP IP Address/Host Name: 10.123.43.111 Port No.: 4651

□ Isolate From All Other Transponders For Location □ Ignore Communications Failure

Trouble Type Text:

Trouble Tamper Text:

Trouble Response Text:

○ Show points
● Show areas

Point or Area Data

Number: 0

□ Virtual fence □ Third floor
□ Second floor □ All above

Alert 1:
Alert 2:
Alert 3:

Pager Group: Floor: Outside

Location:

Map: 0

Figure 4.14: Transponder Area Edit Dialog

Number Each transponder can have up to 80 areas defined in them (prior to version 2.04 of the software, only 40 areas could be defined). This area number range from 0 to 79. Use the **[Locate]** button to define the area graphically on the map.

Video Switcher Selects a system serial port that is programmed in the **Remote Setup** dialog. The purpose is to display the area, where the alarm is most likely located, on the CCTV monitors near the Central Console. The string would activate a macro in the video switcher that selects the appropriate camera, and controls any required zoom and tilt actions. Up to 40 characters may be entered. Control characters may be entered as "^A" for control A.

Pager Group This **Pager Group** field may be programmed with a pager group that is paged if the alarm location is determined to be in this area. This pager group will be the first group paged to allow quick response by those individuals charged with responding to an alarm in this area. Each area may be assigned a pager group that can be the same or different from other alarm areas.
The default alarm **Pager group** defined in the **Pager Setup** dialog will also be paged after the pager group is assigned to an area. If a pager group is not assigned to an area or the alarm location is not within a defined area, then only the default pager group will be paged.

Floor Determines the floor number that this area is defined for. The areas on floors above and below this one may be defined differently. In order for an area to be selected when an alarm is received, the location determined by the Central Console must be located within the defined area, and it must be located on the designated floor.

Virtual Fence Area If this checkbox is checked, this area will not be used for normal alarm area location. This area will only be used to define a “Virtual” fence. Specific transmitters in the **Subscriber Database** can reference this transponder and area. When they reference this area, and the system locates the transmitter position outside the area, a wandering (“Virtual” fence) alarm will be generated. This alerts the operator and shows the position of the transmitter.

4.1.7 Transmitter Change

The **Transmitter Change** menu item is used when it is necessary to change a subscriber’s transmitter. See the Security Escort *Operation Manual*.

4.1.8 Exit

Click the **Exit** menu item to close the Security Escort application. Enter your password at the prompt to verify you have the authority to shut down the program.

4.2 Utilities menu

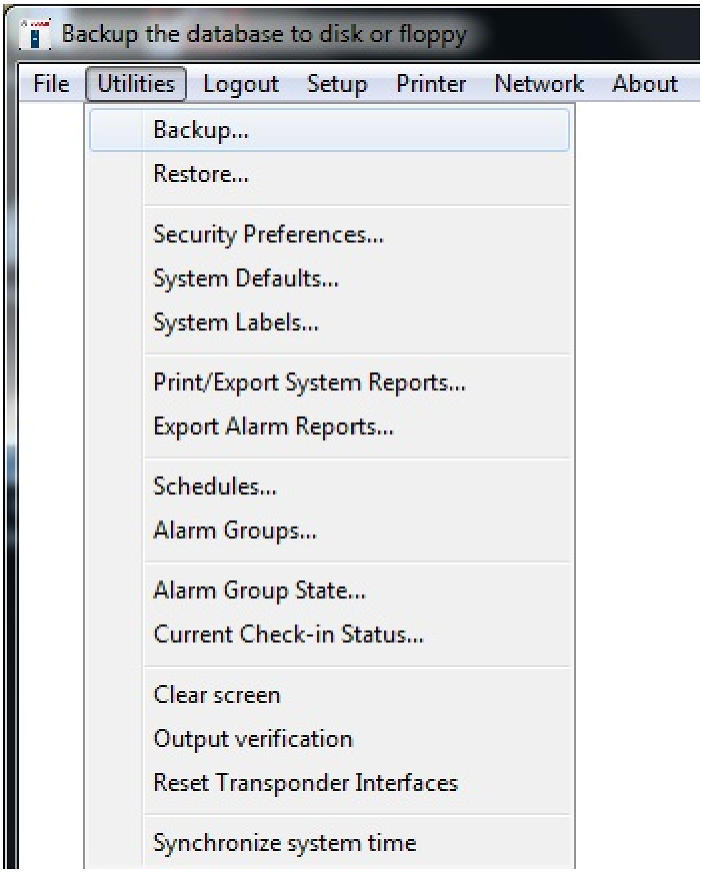


Figure 4.15: Utilities Menu

4.2.1 Backup dialog

This feature provides a convenient process for saving the information in the databases to backup files.

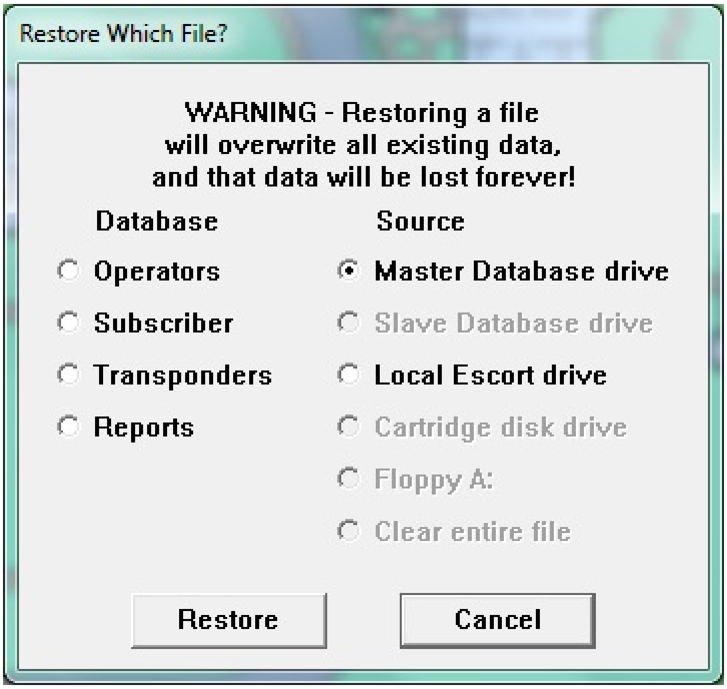
Warning!

To prevent the accidental loss, the databases should be backed up at least once a week to multiple backups. At least one of these backup copies should be kept in a different location from the central console’s location.

Weekly backups are recommended to permit data recovery if the computer memory should become corrupted. If this unlikely event occurs, an operator can quickly restore the databases in question with the **Restore** command. Backups should be made any time significant changes are made to any database.

Notice!

If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the backup properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.



Restore Which File?

WARNING - Restoring a file
will overwrite all existing data,
and that data will be lost forever!

Database
○ Operators
○ Subscriber
○ Transponders
○ Reports

Source
● Master Database drive
○ Slave Database drive
○ Local Escort drive
○ Cartridge disk drive
○ Floppy A:
○ Clear entire file

Figure 4.16: Backup Dialog

When the **Backup** menu item is chosen, options are presented to save the databases to the master or slave computer’s hard drive, a cartridge drive, or to a floppy drive of this computer. When saving to a floppy disk or cartridge drive, verify that the appropriate disk or cartridge is inserted into the drive before clicking the **[Backup]** button. To abort the process, click the **[Cancel]** button in the dialog.
Only the databases with a checkmark will be backed up. Typically all databases should be backed up at once. Only when they do not fit on one floppy disk should you save individual databases to one floppy, then switch floppy disks and repeat the procedure to save the rest of the files. As insurance against database problems, multiple backups to different disks should be made frequently. At least one backup copy should be stored in a different location from this system (remember to keep this copy current).

Operators This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.

Subscriber This database contains all of transmitters assigned in the system.

Transponders This database contains the configuration of the transponders, receivers, virtual receivers and alert units.

Reports This database contains all of the alarm reports and related alarm map screens.

Master Database drive Store the backup files in the Security Escort Master Database path. See the **System Directories and Network Address** dialog.

Slave Database drive Store the backup files in the Security Escort Slave Database path. See the **System Directories and Network Address** dialog.

Local Escort drive Store the backup files in the save sub-directory as the Security Escort System components are stored on this computer (typically C:\ESCORT).

Cartridge disk drive Store the backup files in the **Backup / restore to disk cartridge path** assigned in the **System Preferences** dialog. This path may point to a cartridge disk drive, to a local hard disk or to a network disk drive.

Floppy A: Store the backup files on the floppy disk in floppy disk drive A.

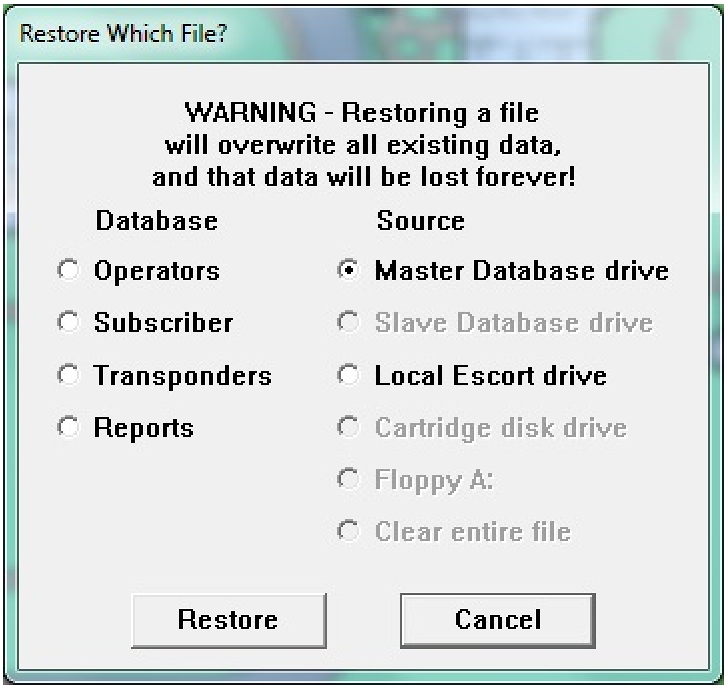
[Backup] When the **[Backup]** button is clicked, all databases selected with a checkmark will be saved to the destination selected on the right.

4.2.2 Restore dialog

Should one or more database files become corrupted or erased due to a hard drive failure, power surges or other unpredictable events, it is necessary to restore the databases from backup files. The **Restore** function allows loading of selected databases from backup files. It is not necessary to perform the **Restore** function on all databases in order to restore any one. All changes that occurred since the last backup are lost when a database is restored. Therefore, restore only those databases with a problem. Backups should be made whenever significant changes are made to any database.

Notice!

If the Security Escort system is configured to share the database, you will need to exit the Security Escort program on all slave and workstation computers. The master computer will not be able to perform the restore properly as other computers are also using the files. The master computer needs to have exclusive use of the database files.



Restore Which File?

WARNING - Restoring a file
will overwrite all existing data,
and that data will be lost forever!

Database	Source
○ Operators	● Master Database drive
○ Subscriber	○ Slave Database drive
○ Transponders	○ Local Escort drive
○ Reports	○ Cartridge disk drive
	○ Floppy A:
	○ Clear entire file

Figure 4.17: Restore Dialog

Select the database to be restored on the left. On the right, this is where the database backup is currently located. Click the **[Restore]** button to replace the existing database file with the backup. This process also rebuilds the database and its index tables to correct most database structure problems. To abort the restore process, click the **[Cancel]** button.

Operators
This is the database of all of the individuals with passwords to operate the system software and acknowledge alarms.

Subscriber
This database contains all of transmitters assigned in the system.

Transponders
This database contains the configuration of the transponders, receivers, virtual receivers and alert units.

Reports
This database contains all of the alarm reports and related alarm map screens.

Master Database drive
Store the backup files in the Security Escort **Master Databasepath**. See the **System Directories and Network Address** dialog.

Slave Database drive
Store the backup files in the Security Escort **Slave Databasepath**. See the **System Directories and Network Address** dialog.

Local Escort drive
Store the backup files in the save sub-directory as the Security Escort System components are stored on this computer (typically “C:\ESCORT”).

Cartridge disk drive
Store the backup files in the Backup / restore to disk cartridge path assigned in the **System Preferences** dialog. This path may point to a cartridge disk drive, to a local hard disk or to a network disk drive.

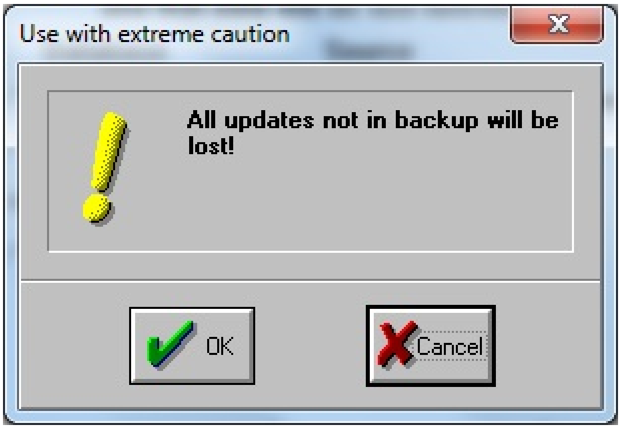
Floppy A
Store the backup files on the floppy disk in floppy disk drive A.

Clear entire file

If selected and the **[Restore]** button clicked, then that entire database will be cleared of all records. This selection must be used with extreme caution! Hold down the <Shift>+<Ctr;> keys when opening the dialog to enable the **Clear entire file** option.

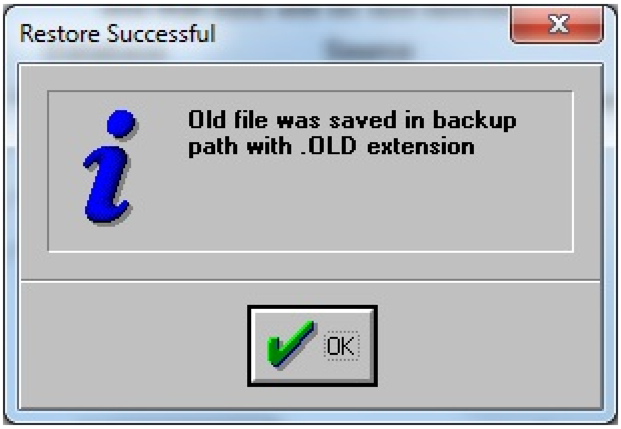
[Restore]

When the **[Restore]** button is clicked the database selected will be restored from the destination selected on the right.


Use with extreme caution

All updates not in backup will be lost!

This message box is a reminder that if changes to the system databases have been made since the backup was made, the changes will be lost. Therefore those changes must be redone to the restored database.

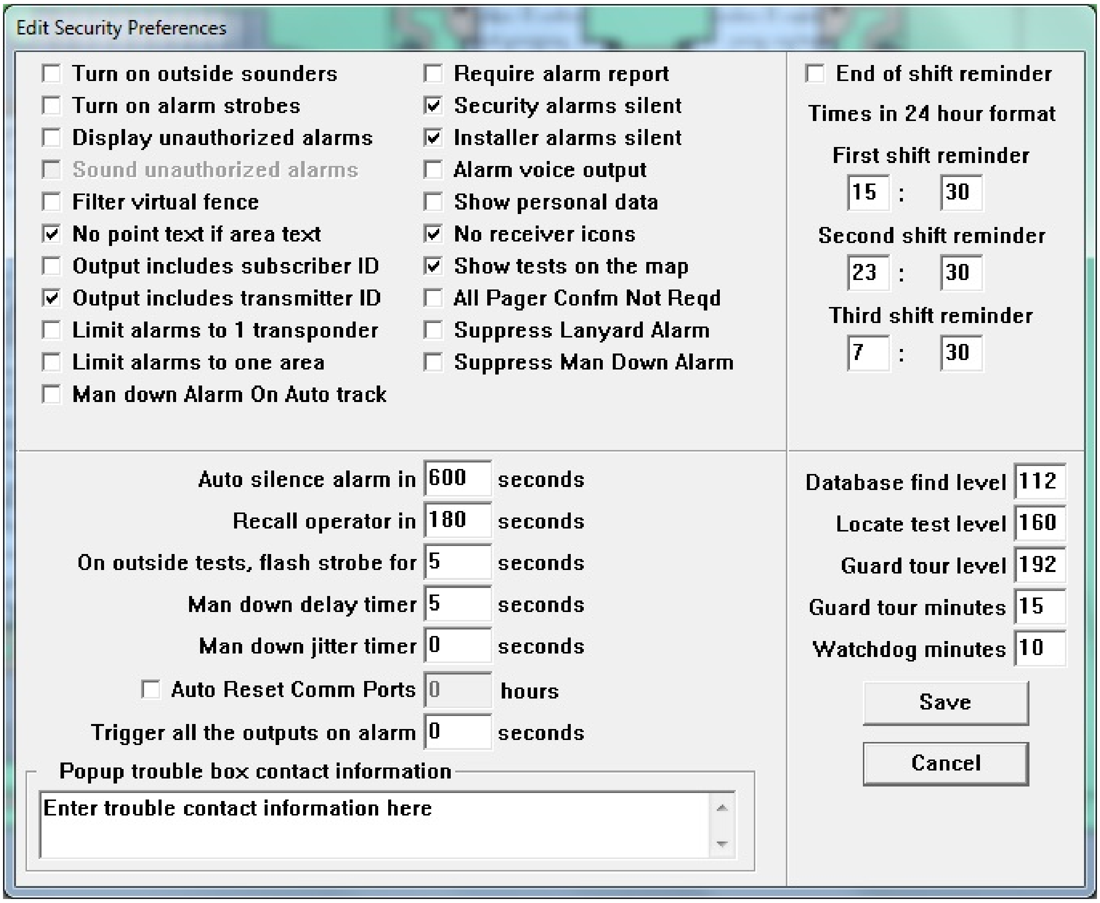

Restore Successful

Old file was saved in backup path with .OLD extension

This message box indicates the restore has been completed. The previous database file has been renamed with an .OLD extension and saved in the Escort sub-directory. Only the most recent database of each type is retained.

4.2.3 Security Preferences dialog

The **Security Preferences** dialog is used to make important settings that govern how the Security Escort System reacts in the event of alarm and test transmissions from the subscribers' transmitters. This dialog is available only to the Security Director or his/her key operator.



Edit Security Preferences

☐ Turn on outside sounders
☐ Turn on alarm strobes
☐ Display unauthorized alarms
☐ Sound unauthorized alarms
☐ Filter virtual fence
☑ No point text if area text
☐ Output includes subscriber ID
☑ Output includes transmitter ID
☐ Limit alarms to 1 transponder
☐ Limit alarms to one area
☐ Man down Alarm On Auto track

☐ Require alarm report
☑ Security alarms silent
☑ Installer alarms silent
☐ Alarm voice output
☐ Show personal data
☑ No receiver icons
☑ Show tests on the map
☐ All Pager Confm Not Reqd
☐ Suppress Lanyard Alarm
☐ Suppress Man Down Alarm

☐ End of shift reminder
Times in 24 hour format
First shift reminder 15 : 30
Second shift reminder 23 : 30
Third shift reminder 7 : 30

Auto silence alarm in 600 seconds
Recall operator in 180 seconds
On outside tests, flash strobe for 5 seconds
Man down delay timer 5 seconds
Man down jitter timer 0 seconds
☐ Auto Reset Comm Ports 0 hours
Trigger all the outputs on alarm 0 seconds

Popup trouble box contact information
Enter trouble contact information here

Database find level 112
Locate test level 160
Guard tour level 192
Guard tour minutes 15
Watchdog minutes 10

Figure 4.18: Security Preferences Dialog

Most of the options given are simple checkboxes. To activate or deactivate the option given, click on the checkbox adjacent to the text. A check mark appears in the checkbox adjacent to activated option, empty checkboxes signify deactivated options. Some options in the **Security Preferences** dialog require numerical values. To change the current values, click the text box containing the values, then type in a new value.
Clicking the **[Save]** button saves the modifications and exits the **Security Preferences** dialog. Click the **[Cancel]** button to save the changes made so far, to discard the changes, or to remain in the **Security Preferences** dialog.

Turn on outside sounders This checkbox is used to activate or deactivate the sirens on alert units and transponders. Some security directors prefer that all alarms be silent, others choose to employ sirens. Checking this option causes the sirens on the alert units, to sound in the event of an alarm. Temporarily deactivating the sounders may be necessary during maintenance.

Turn on alarm strobes Checking this option causes the strobe lights on the alert units and transponders, to flash in the event of an alarm.

Display unauthorized alarms

This checkbox determines if “unauthorized" alarms are to be displayed on the Central Console. Unauthorized alarms are those triggered by transmitters not currently registered in the **Subscriber Database**. These could be transmitters that have been removed from the database because they were lost or stolen, they could be transmitters not yet issued, or they could be transmitters issued to subscribers at another Security Escort System. Typically this checkbox should not be checked.

Sound unauthorized alarms

This checkbox determines if "unauthorized” alarms are to be sounded on the horns of the receivers and the sirens of the alert units and transponders. The option is not available unless the **Display unauthorized alarms** option is selected. Typically this checkbox should not be checked.

Filter virtual fence

If the virtual fence option is be used, this box may be checked if some false alarms are generated to reduce the number of the false alarms. If it is checked then the actual alarms will be delayed by the supervision period of the transmitter.

No point text if area text

This checkbox affects the location text shown on the alarm screen. If this checkbox is checked and the alarm is determined to be within a predefined area then only the area text will be displayed (any receiver location text will be suppressed). Typically this checkbox should be checked.

Output includes subscriber ID

If this checkbox is checked, then any time the system prints or displays text for an alarm or test the subscriber’s ID number will also be displayed. Otherwise the subscriber’s ID will not be shown.

Output includes transmitter ID

If this checkbox is checked, then any time the system prints or displays text for an alarm or test the transmitter ID number will also be displayed. Otherwise the transmitter ID will not be shown. Typically this checkbox would not be checked.

Limit alarms to 1 transponder

This checkbox should not be checked. It was used only in a system where all transponders operate on areas that are separate from each other. It would prevent all interactions between receivers on different transponders. Typically this would be very undesirable and there is now a selection on an individual transponder basis to accomplish this feature.

Limit alarms to one area

This checkbox should not be checked. It is used only in a system where all transponders operate on areas that are separate from each other.

Man down Alarm On Auto track

If this checkbox is checked, then any time there is a man down alarm, the auto track functionality will be activated. Otherwise there is no auto track functionality for the alarm.

Require alarm report
If this checkbox is checked, the operator will be prompted to complete an alarm report when the alarm is reset from the screen. If the responding officer is required to complete the report, or if no system report is desired, this box should not be checked. If the operator should complete the report then check this box.

Security alarms silent
If this checkbox is checked, then alarms transmitted by security or watchman transmitters are to be silent, alerting the operator at the Central Console, but not sounding the sirens of the alert units or the horns in the receivers.

Installer alarms silent
If this checkbox is checked, then alarms transmitted by transmitters issued to installing company representatives and visitors are to be silent, alerting the operator at the Central Console, but not sounding the sirens of the alert units or the horns in the receivers. Typically this checkbox would be checked.

Alarm voice output
If this checkbox is checked, then predefined sound (.WAV) files can be played at the alarm console for specific alarm types. Typically this checkbox would not be checked.

Show personal data
If this checkbox is checked, then personal height, build, hair and eye color data will be displayed on the alarm screen.

No receiver icons
If this checkbox is checked, then individual receiver icons will not be shown on the alarm map display. Typically this checkbox would be checked.

Show tests on the map
If this checkbox is checked, tests from subscriber's transmitter will be displayed on the normal map screen as **OK** or **FAIL** icons, signifying a successful test by a valid subscriber or an attempted test transmission from a transmitter not in the **Subscriber Database**. This option doesn’t affect the display the subscriber receives from a receiver or alert unit’s strobe. Typically this checkbox would be checked.

All Pager Confm Not Reqd
If this checkbox is checked, the confirmation pager message is not sent to the any of the pagers when the alarm is acknowledged by an acknowledgement transmitter.

Suppress Lanyard Alarm
If this checkbox is checked, the lanyard alarm is suppressed and not reported.

Suppress Man Down Alarm
If this checkbox is checked, the man down alarm is suppressed and not reported.

Auto silence alarm in 'X' seconds
This box determines the length of time that the sirens and horns will sound before being automatically silenced by the Central Console. When the sounders are automatically silenced in this way, the Central Console remains in its alarm mode. The numerical value is in seconds, and it can be set between 0 and 9999. Typically this value would be set to prevent violating local noise ordinances and it defaults to 240 seconds (4 minutes).

Recall operator in 'X' seconds

This box determines the length of time before a recall alert is issued to the operator at the Central Console when an alarm is being displayed. If neither the mouse nor any key has been actuated for the specified length of time, the Central Console will trigger the alarm sound once. This feature prevents inadvertently ignoring an active alarm event. The numerical value is in seconds, and it can be set between 0 and 240. Typically this would be set to 60 seconds.

On outside tests, flash strobe for 'X' seconds

The entry in this box controls the approximate length of time the strobe on an alert unit will flash to signify a successful transmitter test. The value is in seconds, and can be set between 0 and 15. Typically it is set to 5 seconds.

Man down delay timer ‘X’ seconds

This value controls the time that a transmitter must be in a man down condition before a man down alarm is displayed. Typically it would be set to 10 seconds. Setting this value too short will cause inadvertent man down alarms to be generated.

Man down jitter timer ‘X’ seconds

This value controls the time that a transmitter will not be considering any man down alarm if man down alarm is received immediately after restore and before jitter time expire. This setting will not be used in normal system.

Auto Reset Comm Ports ‘X’ hours

This value controls the time that all the comm ports in the system will be automatically reset after configured duration. This setting is used only if any communication failure is observed and should not be used unnecessarily.

Trigger all the outputs on alarm ‘X’ seconds

This option turns on all outputs of the transponders, and alert units for the duration configured (1-255 seconds) when alarm is generated. If someone acknowledges an alarm during this duration, all these outputs will be turned off. Otherwise, after this duration has lapsed, all these outputs will be turned off automatically. If this value is set to 0, the system will trigger the outputs during alarms in the default normal behavior.

End of shift reminder

A check in this checkbox causes a prompt to appear on the Central Console screen every 5 minutes for 30 minutes prior to the end of each shift if there are incident reports that have not yet been completed. It is intended for responding officers to complete alarm reports before the end of their shift.

First, Second, Third shift reminder

The entries in these fields are the times (24-hour clock) at which the Central Console will prompt the operator that there is one or more incident reports that have not yet been completed. Prompts will be given only if the **End of Shift Reminder** option is selected.

Database find level

This is the minimum receive level (1-255) that must be heard before the system will automatically enter the transmitter in the **Subscriber Locate** dialog. It determines the distance the subscriber’s transmitter must be within the specified ID capture receiver (set in the **System Preferences** dialog) before the system will recognize the test.

Locate test level This is the minimum receive level (1-255) that must be heard before the system will accept a test generated by a transmitter other than a guard, to be printed with a location. It determines the distance the transmitter must be within from a receiver before the system will recognize the test and print the location. If the transmitter is too far away from the receiver, that receiver’s green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.

Guard tour level This is the minimum receive level (1-255) that must be heard before the system will accept a test generated by the guard’s transmitter to be entered as a location in the guard tour report. It determines the distance the guard’s transmitter must be within from a receiver before the system will recognize the test and create the guard tour entry. If the guard is too far away from the receiver, that receiver’s green light will not be displayed, so the guard knows that they must move closer to the receiver for the test to register.

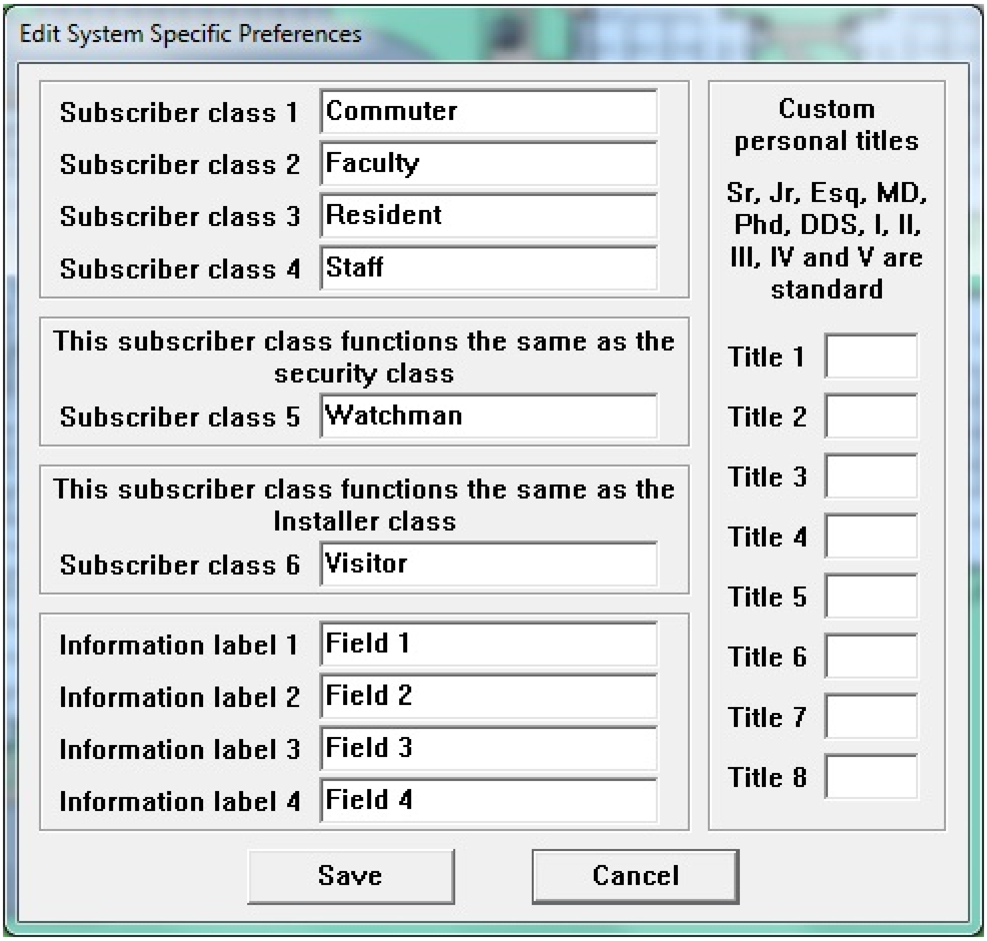
Guard tour minutes This setting controls the time spacing, in minutes, for entries of the guard’s current location in the automatically generated guard tour report. Therefore if set to 15 minutes, an entry will be generated each 15 minutes that the guard’s transmitter is within range of the system.

Watchdog minutes This setting controls the time spacing, in minutes, for entries of the guard’s current location in the automatically generated guard tour report. Therefore if set to 15 minutes, an entry will be generated each 15 minutes that the guard’s transmitter is within range of the system.

Popup trouble box contact information” Each yellow, pop-up trouble box that is displayed on the Central Console advises of system problems, containing specific instructions for the operator. Entries in this text box will be displayed in the pop-up trouble boxes whenever a system problem occurs that requires attention. This information usually includes the name and telephone number of the designated Security Escort maintenance technicians.

4.2.4 System Defaults dialog

This dialog allows the names for each class of subscribers to be changed to match the specific application of this Security Escort System.



Edit System Specific Preferences

Subscriber class 1: Commuter

Subscriber class 2: Faculty

Subscriber class 3: Resident

Subscriber class 4: Staff

This subscriber class functions the same as the security class

Subscriber class 5: Watchman

This subscriber class functions the same as the Installer class

Subscriber class 6: Visitor

Information label 1: Field 1

Information label 2: Field 2

Information label 3: Field 3

Information label 4: Field 4

Custom personal titles

Sr, Jr, Esq, MD, Phd, DDS, I, II, III, IV and V are standard

Title 1:

Title 2:

Title 3:

Title 4:

Title 5:

Title 6:

Title 7:

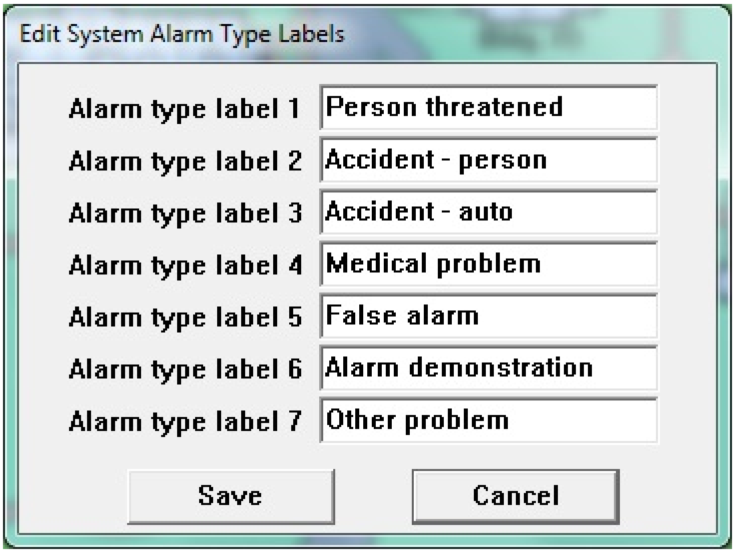
Title 8:

Figure 4.19: System Defaults Dialog

Titles that are entered into the **Subscriber Name** field in the **Subscriber Database** are entered here. The system alphabetizes the **Subscriber Database** entries by last name. When a title is entered after the last name, the entry is alphabetized incorrectly by title. Entering the titles prevents this problem.
The labels for the four **Information label** in the **Subscriber Database** are also changeable here.

4.2.5 System Labels dialog

The alarm type definitions are customized to customer’s requirements in this dialog window.

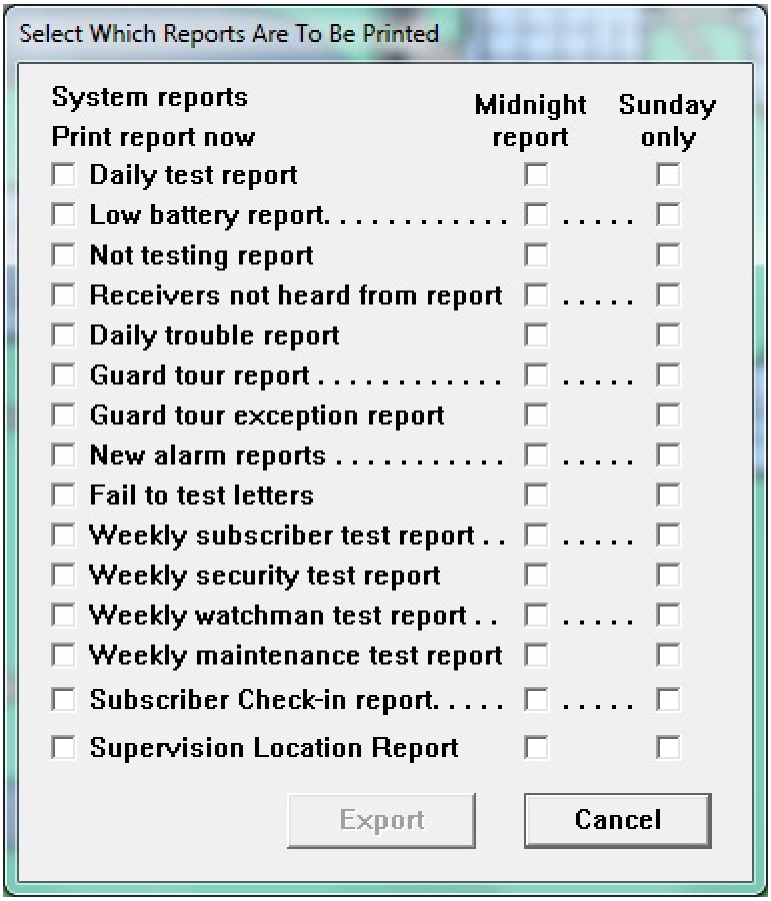


Alarm type label 1	Person threatened
Alarm type label 2	Accident - person
Alarm type label 3	Accident - auto
Alarm type label 4	Medical problem
Alarm type label 5	False alarm
Alarm type label 6	Alarm demonstration
Alarm type label 7	Other problem

Figure 4.20: System Label Dialog

4.2.6 Print/Export System Reports dialog

This dialog allows the system reports to be printed on demand, scheduled for printing each night at midnight or weekly on Sunday at midnight. To print a report, select the left-checkbox for each desired report and click the **[Print]** button. Select the **Midnight report** or the **Sunday only** checkboxes to automatically schedule the selected report at those times.



System reports Print report now	Midnight report	Sunday only
☐ Daily test report	☐	☐
☐ Low battery report.	☐	☐
☐ Not testing report	☐	☐
☐ Receivers not heard from report	☐	☐
☐ Daily trouble report	☐	☐
☐ Guard tour report	☐	☐
☐ Guard tour exception report	☐	☐
☐ New alarm reports	☐	☐
☐ Fail to test letters	☐	☐
☐ Weekly subscriber test report . .	☐	☐
☐ Weekly security test report	☐	☐
☐ Weekly watchman test report . .	☐	☐
☐ Weekly maintenance test report	☐	☐
☐ Subscriber Check-in report.	☐	☐
☐ Supervision Location Report	☐	☐

Figure 4.21: Print/Export System Reports Dialog

Daily test report
Report of testing by classes of subscriber for the last 24 hours broken down by hour.

Low battery report
Report of all subscriber transmitters currently reporting low battery.

Not testing report
Report of all subscriber transmitters that have not tested their transmitters within the last 28 days.

Receivers not heard from report
Report of all receivers that have not heard transmissions recently. This could indicate a problem with the receiver’s ability to hear alarms and test transmissions.

Daily trouble report
Report of all the troubles currently being reported by transponders, receivers and alert units.

Guard tour report
Report of the guard tours collected within the last day. This selection does not generate a printed report. However, the **Midnight report** and **Sunday only** checkboxes must be checked to write a file of the guard tour information. Another application like Microsoft Excel can sort and print the desired reports.

Guard tour exception report
The guard tour exception reports collected within the last day. Not currently implemented.

New alarm reports
Alarm reports for all of the new alarms that have been received by the system.

Fail to test letters
Notices to all of the subscribers that have not tested within the last 28 days. Not currently implemented.

Weekly subscriber test report
Report of subscriber testing for the last 7 days broken down by hour.

Weekly security test report
Report of security personnel testing for the last 7 days broken down by hour.

Weekly watchman test report
Report of watchman personnel testing for the last 7 days broken down by hour.

Weekly maintenance test report
Report of maintenance testing for the last 7 days broken down by hour.

Subscriber Check-in report
Report of all subscribers that failed to check-in during the last scheduled check-in period.

Supervision Location report
Report of all supervision enabled subscribers and their last known location.

[Print]
Clicking this button prints all reports that are checked in the left-hand check boxes.

[Export]
Clicking this button exports all reports that are checked in the left-hand checkboxes.

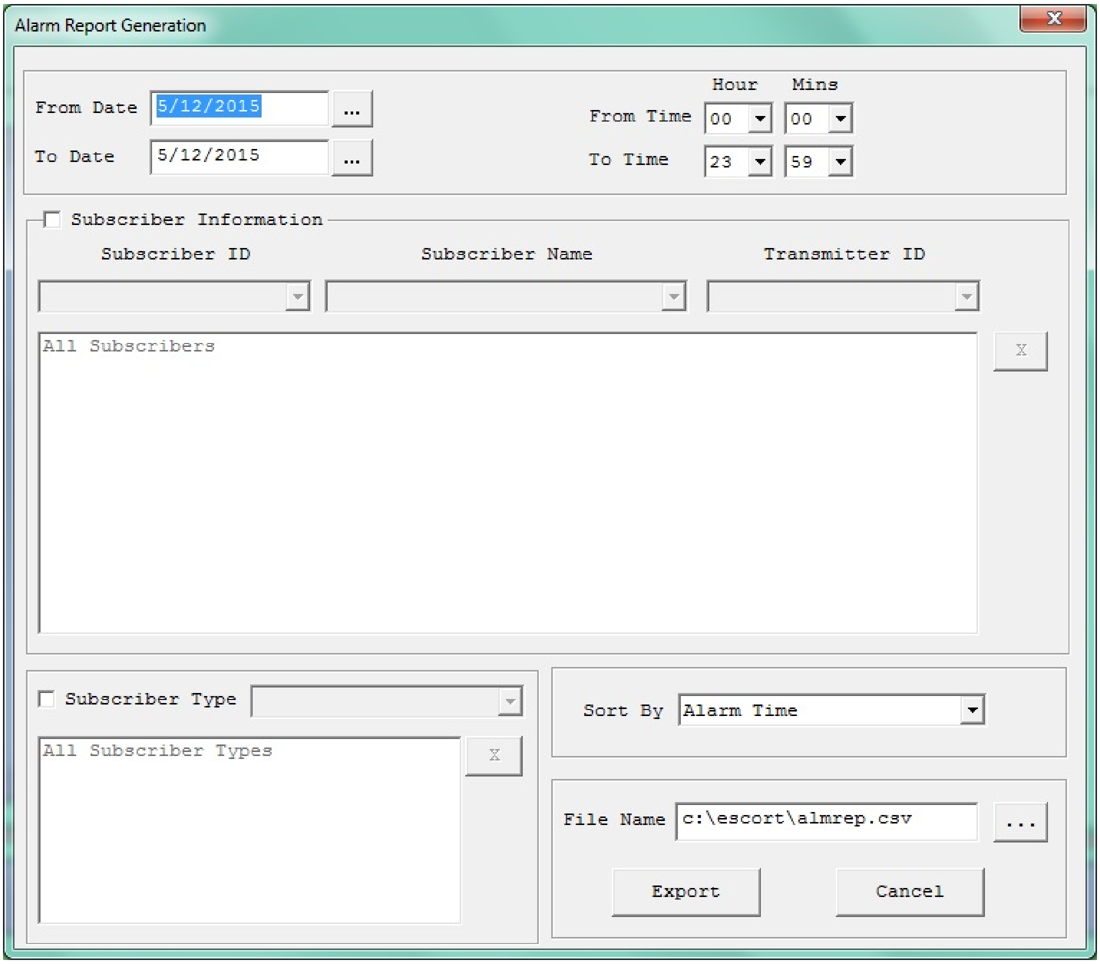
Print report now
Reports that are selected are printed when the **Print** button is clicked.

Midnight report
Reports are automatically generated every midnight for all reports that are checked in the **Midnight report** checkboxes.

Sunday report
Reports are automatically generated every Sunday at midnight for all reports that are checked in the **Sunday report** checkboxes.

4.2.7 Export Alarm Reports dialog

This dialog allows the alarm reports to be exported to CSV file. To export an alarm report, you may directly enter the alarm date range, or click the **[...]** (ellipsis) button in **From Date**, **To Date** fields and select **From Time**, **To Time** from the respective drop-down values. An alarm report can also be generated based on the subscriber details. Select the **Subscriber ID**, **Subscriber Name**, **Transmitter ID** or **Subscriber Type** from the drop down list to generate an alarm report only for the selected values.



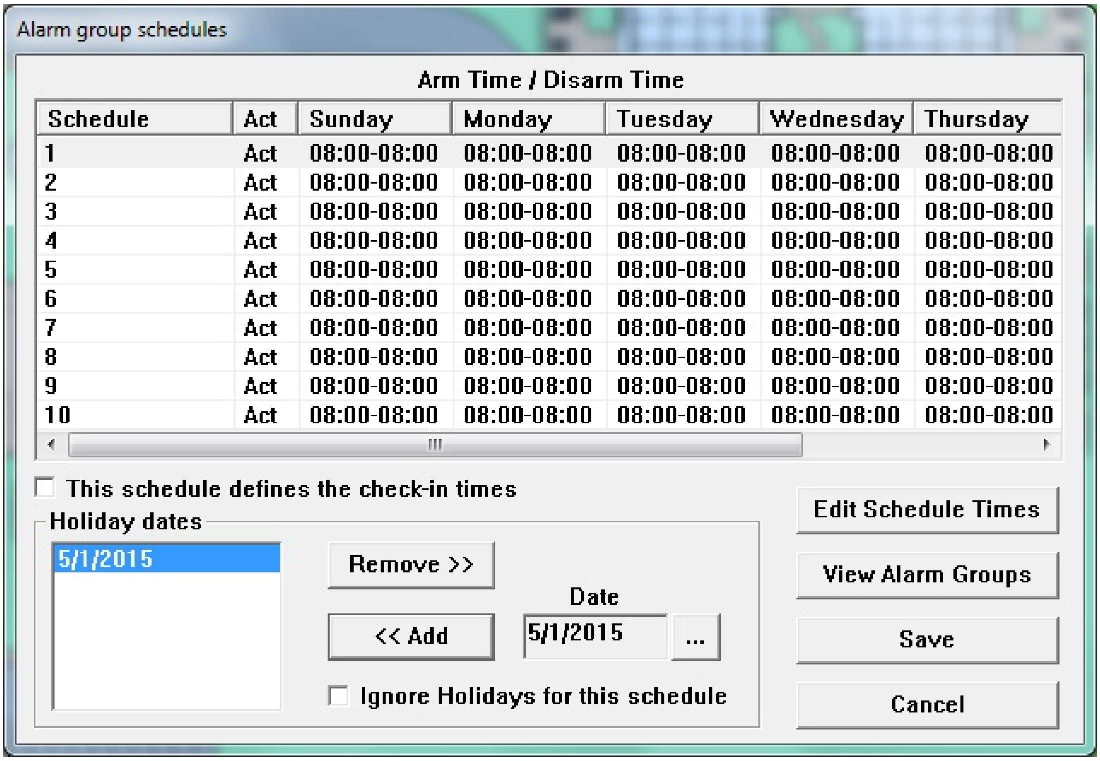
From Date 5/12/2015
To Date 5/12/2015
From Time 00 00
To Time 23 59
□ Subscriber Information
All Subscribers
□ Subscriber Type
All Subscriber Types
Sort By Alarm Time
File Name c:\escort\almrep.csv

Figure 4.22: Export Alarm Report

The alarm report can be sorted by **Alarm Time**, **Transmitter ID**, **Subscriber Name**, **Problem Type**, **Subscriber Type**, by using the **Sort By** drop-down list. You can change the report name and file location by pressing the **[...]** (ellipsis) button. Clicking the **[Export]** button saves the report to the specified file. Clicking the **[Cancel]** button cancels the report generation and exits from the dialog window.

4.2.8 Schedules dialog

This selection informs management of the ten-time of day/day of week schedules and holidays. The top portion of the display shows the ten-time-of-day/day-of-week schedules that Security Escort supports. For each schedule, there is an indication the schedule is currently active or armed (ACT); otherwise, the schedule is disarmed (OFF).



Alarm group schedules

Arm Time / Disarm Time

Schedule	Act	Sunday	Monday	Tuesday	Wednesday	Thursday
1	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
2	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
3	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
4	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
5	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
6	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
7	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
8	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
9	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00
10	Act	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00	08:00-08:00

□ This schedule defines the check-in times

Holiday dates: 5/1/2015

Date: 5/1/2015

□ Ignore Holidays for this schedule

Figure 4.23: Schedule Screen

For each day-of-the-week, the arm time (time the schedule becomes active) and disarm time (time the schedule becomes inactive) are displayed. To edit the arm and disarm times, click the **[Edit Schedule Times]** button. Double clicking the number of the schedule allows you to name the schedules.

This schedule defines the check-in times
One of the ten schedules can be used to define the check-in times for those subscribers that must check-in. Click on the schedule for the check-in schedule, highlighting it. Then check this checkbox, to set the selected schedule as the check-in schedule. Both the arm time and disarm time must be programmed for every day the check-ins must take place. The arm time is the start of the check-in schedule and it must occur before the disarm time that marks the end of the check-in schedule for that day.

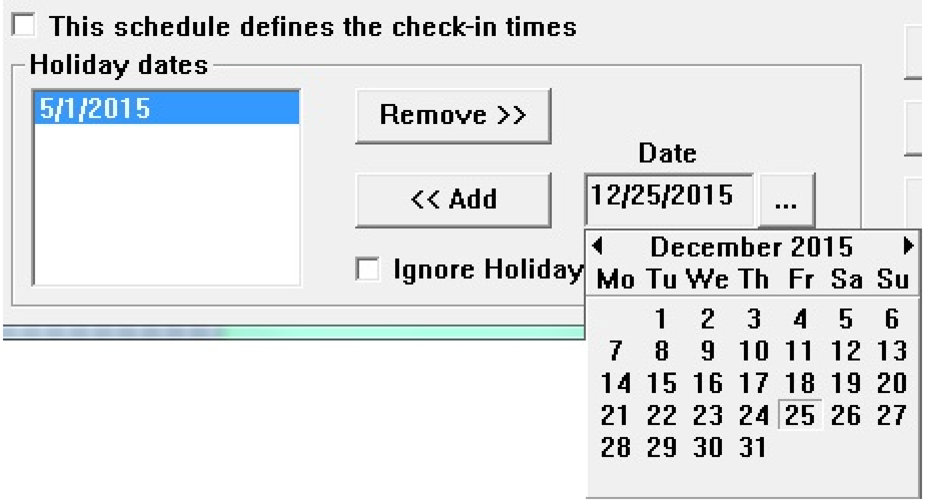
[Edit Schedule Times]
Clicking this button displays the **Edit Schedule Times** dialog so the day of week arm and disarm schedule times can be edited.

[View Alarm Groups]
Clicking this button displays the **View Alarm Groups** dialog. This screen shows the alarm groups assigned to the selected schedule and their current arming state.

Ignore Holidays for this Schedule
Each schedule can use the holiday dates as exceptions.

Ignore Holidays for this schedule option

Each schedule can use the holiday dates as exceptions. Schedules are activated (armed) following the normal schedules if the holiday dates are configured to be ignored. Otherwise, the schedules are activated the entire day for the holiday dates.



☐ This schedule defines the check-in times

Holiday dates: 5/1/2015

Date: 12/25/2015

☐ Ignore Holiday

Mo	Tu	We	Th	Fr	Sa	Su
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Figure 4.24: Holiday Selection in the Schedule Dialog

Ignore Holidays for this Schedule If the **Ignore Holidays** checkbox is checked for the indicated holiday dates, the schedules are activated (armed) that entire day. If the **Ignore Holidays** checkbox is not checked, the normal action of the schedules takes place on the holiday dates.

Date [...] Clicking this button displays a calendar where you can graphically select a date.

[Remove >>] Clicking this button removes the selected date from the **Holiday dates** list box.

[<< Add] Clicking this button adds the date shown to the **Holiday dates** list box.

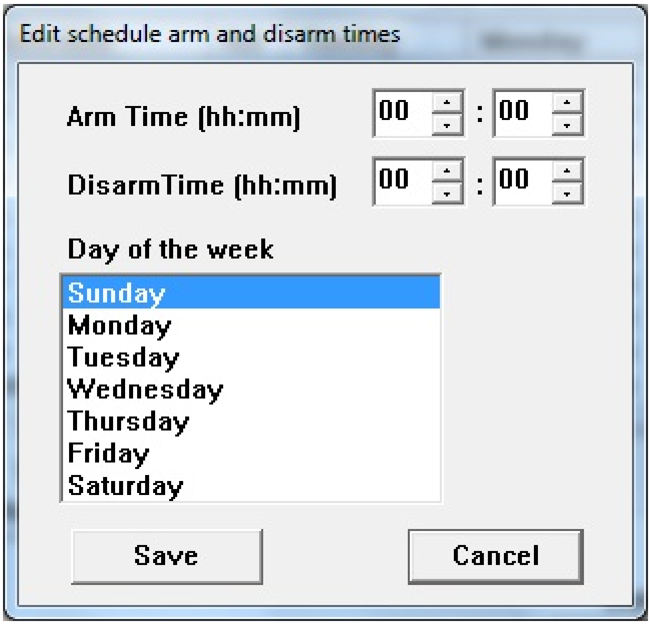
Edit Schedule Times dialog

This dialog allows the arming and disarming times to be programmed for each of the days of the week. All times are expressed in 24-hour time (00:00 to 23:59). Each schedule has one **Arm Time** and one **Disarm Time** for each of the 7 days of the week.

If both the **Arm Time** and **Disarm Time** are programmed to 00:00, the schedule will be active (armed) for the entire day.

If the **Arm Time** is 00:00 and the **Disarm Time** is programmed, the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the end of the day.

If the **Disarm Time** is 00:00 and the **Arm Time** is programmed, the schedule will be off (disarmed) from midnight to the programmed **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.



Edit schedule arm and disarm times

Arm Time (hh:mm) 00 : 00

DisarmTime (hh:mm) 00 : 00

Day of the week: Sunday

Figure 4.25: Edit Schedule Time dialog

If both the **Disarm Time** and the **Arm Time** are programmed, and the **Disarm Time** occurs before the **Arm Time** (normal 8 to 5 style day), the schedule will be active (armed) from midnight to the programmed **Disarm Time**. The schedule will be off (disarmed) from the **Disarm Time** to the **Arm Time**. The schedule will be active (armed) from the **Arm Time** to the end of the day.

If both the **Disarm Time** and the **Arm Time** are programmed, and the **Arm Time** occurs before the **Disarm Time**, the schedule is off (disarmed) from midnight to the programmed **Arm Time**. The schedule is active (armed) from the **Arm Time** to the **Disarm Time**. The schedule is off (disarmed) from the **Disarm Time** to the end of the day.

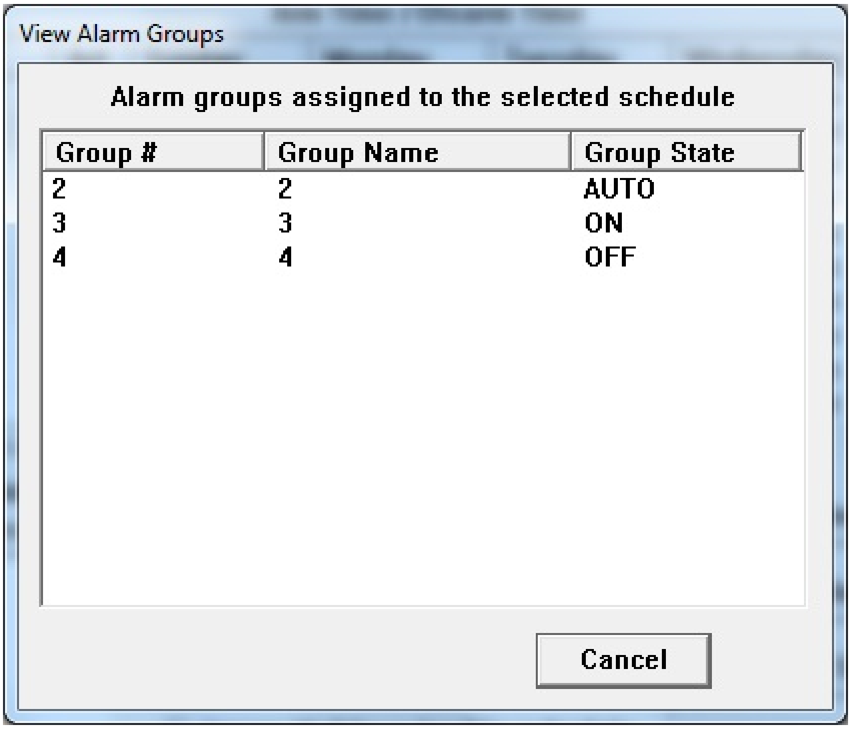
Arm Time This is the time that the schedule becomes active (on or armed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).

Disarm Time This is the time that the schedule goes off (disarmed) for the selected day of the week. Times are expressed in 24-hour time (00:00 to 23:59).

Day of the Week Select the day you desire to change the time for. The **Arm Time** and **Disarm Time** are programmed separately for each day of the week. You must individually select each day of the week, and set the desired times.

View Alarm Groups dialog

This dialog shows the alarm groups that are assigned to the selected schedule and their current arming state. The “ON” and “OFF” states indicate that the alarm group is under manual control. “AUTO” is under control of the selected schedule. The alarm group will be armed if the schedule is active.



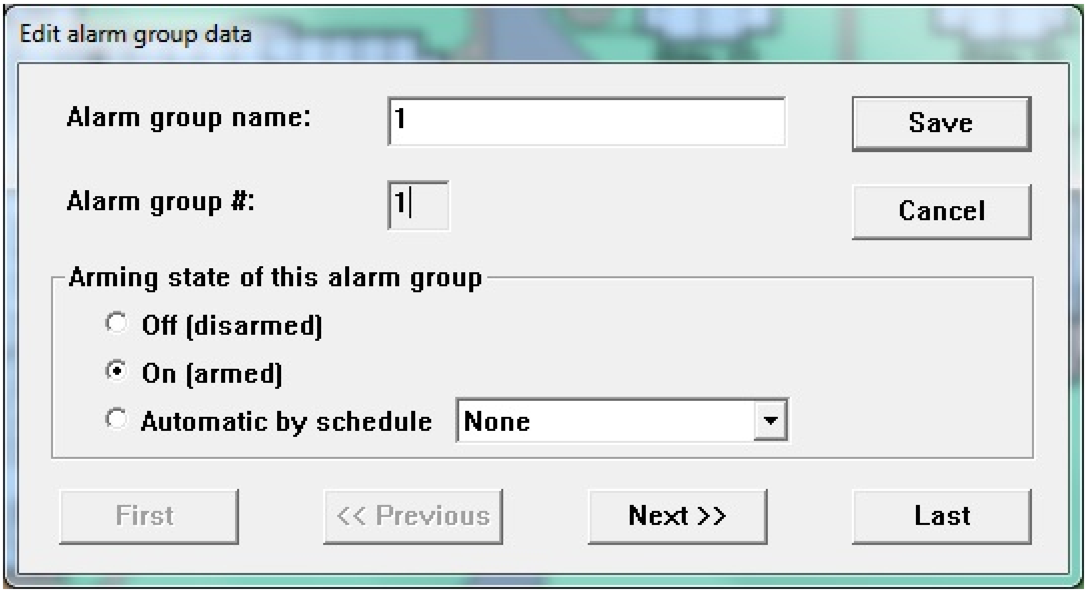
Alarm groups assigned to the selected schedule

Group #	Group Name	Group State
2	2	AUTO
3	3	ON
4	4	OFF

Figure 4.26: View Alarm Groups Dialog

4.2.9 Alarm Groups dialog

This dialog allows setup and arm/disarm control of the 99 alarm groups. Any number of point type transmitters can be assigned to an alarm group in the **Subscriber Database's Advanced** dialog. However, each transmitter can only be assigned to one alarm group.
An alarm group can be manually armed and disarmed, or assigned to a schedule to automatically arm and disarm the alarm group.



Alarm group name: 1

Alarm group #: 1

Arming state of this alarm group

○ Off (disarmed)

● On (armed)

○ Automatic by schedule None

Figure 4.27: Alarm Groups Dialog

Alarm group name Enter a descriptive name to identify the function of the points in this alarm group.

Alarm group # This is the number of the alarm group (1-99).

Arming state of this alarm group The **Off (disarmed)**, **On (armed)** and **Automatic by Schedule** selection control the arming state of this alarm group.

Off (disarmed) Selecting this option disarms the alarm group. The alarm group will remain off (disarmed) until manually changed in this dialog to **On (armed)** or **Automatic by Schedule**.

On (armed) Selecting this option arms the alarm group. The alarm group will remain on (armed) until manually changed in this dialog to **Off (disarmed)** or **Automatic by Schedule**.

Automatic by schedule Selecting this option assigns the alarm group’s arming state to be controlled by the indicated schedule. When the schedule is active (on or armed) the alarm group will be armed. When the schedule is off (disarmed) the alarm group will be disarmed. Any number of alarm groups may be assigned to the same schedule.

[First] Clicking this button takes you to alarm group 1.

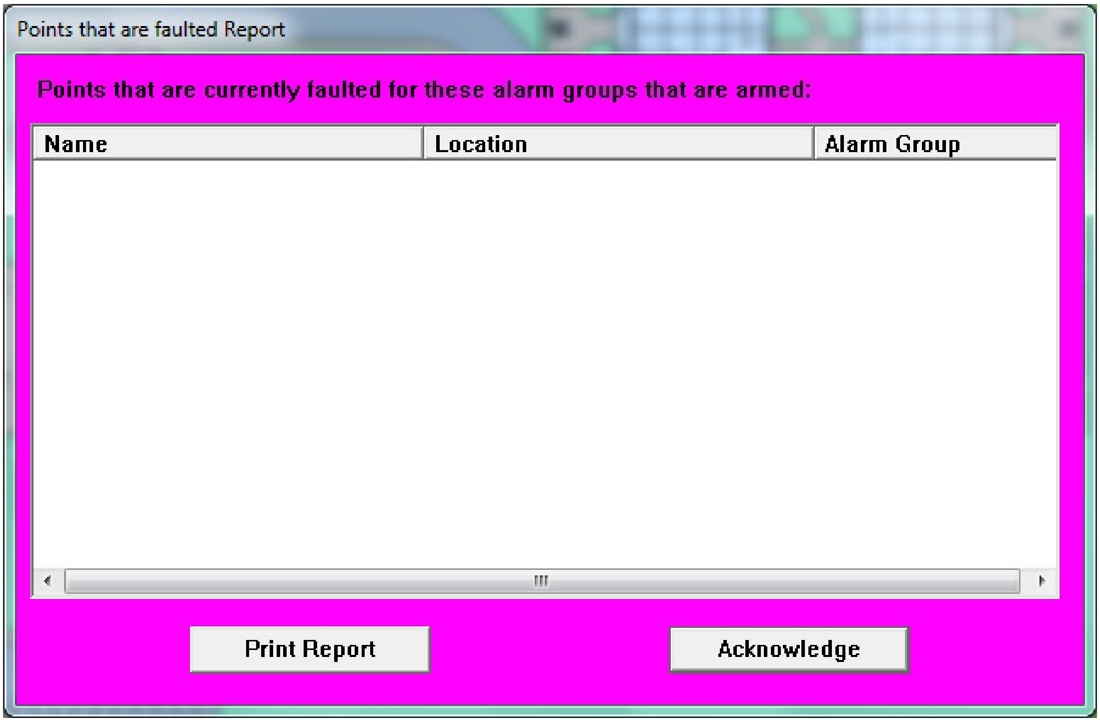
[Previous] Clicking this button takes you to the next lower alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 1.

[Next] Clicking this button takes you to the next higher alarm group from the one currently displayed. It will not wrap around. Therefore, it will be disabled at alarm group 99.

[Last] Clicking this button takes you to alarm group 99.

4.2.10 Alarm Group State dialog

This dialog will display a list of the alarm groups that are currently armed, and have one or more transmitters (points) faulted. The points are presented because they were not restored when their automatic schedule armed, or there was an alarm while the alarm group was on.


Points that are faulted Report

Points that are currently faulted for these alarm groups that are armed:

Name	Location	Alarm Group

Figure 4.28: Alarm Group State Dialog

[Print Report] Clicking this button prints the displayed data to the report printer.

[Acknowledge] Clicking this button closes the dialog if it was selected from the menu. However, if the dialog was presented automatically at the arm time of an alarm group's automatic schedule because they were not restored, or there was an alarm while the alarm group was on, then you are required to enter your password to acknowledge the dialog, and remove it from this computer's (and all other computer workstations) screens.

4.2.11 Current Check-in Status dialog

This dialog displays a list of subscribers that are required to check-in and failed to do so during the last check-in period. Also shown are their addresses, phone numbers, and the last time they checked-in.

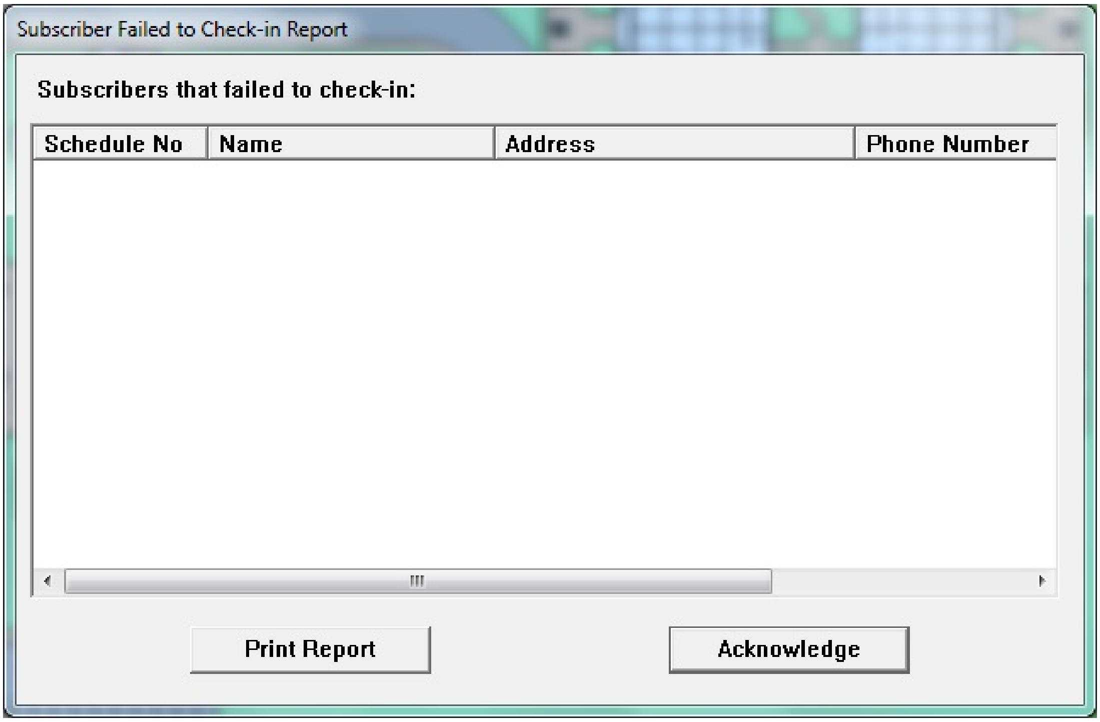

Subscriber Failed to Check-in Report
Subscribers that failed to check-in:
Schedule No
Name
Address
Phone Number
Print Report
Acknowledge

Figure 4.29: Current Check-in Status Dialog

[Print Report] Clicking this button prints the displayed data to the report printer.

[Acknowledge] Clicking this button closes the dialog if it was selected from the menu. However, if the dialog appeared automatically at the end of the check-in period because some subscribers failed to check-in, you must enter your password to acknowledge the dialog and remove it from this computer's (and all other computer workstations) screens.

4.2.12 Clear screen

To clear the screen of any outdated or unwanted data, choose this feature from the **Utilities** menu. The screen automatically resets to its normal operations mode.

4.2.13 Output verification

When selected, the system is scanned to verify that all alarm outputs are in the correct state. Any output found in the wrong state is corrected.

4.2.14 Synchronize system time

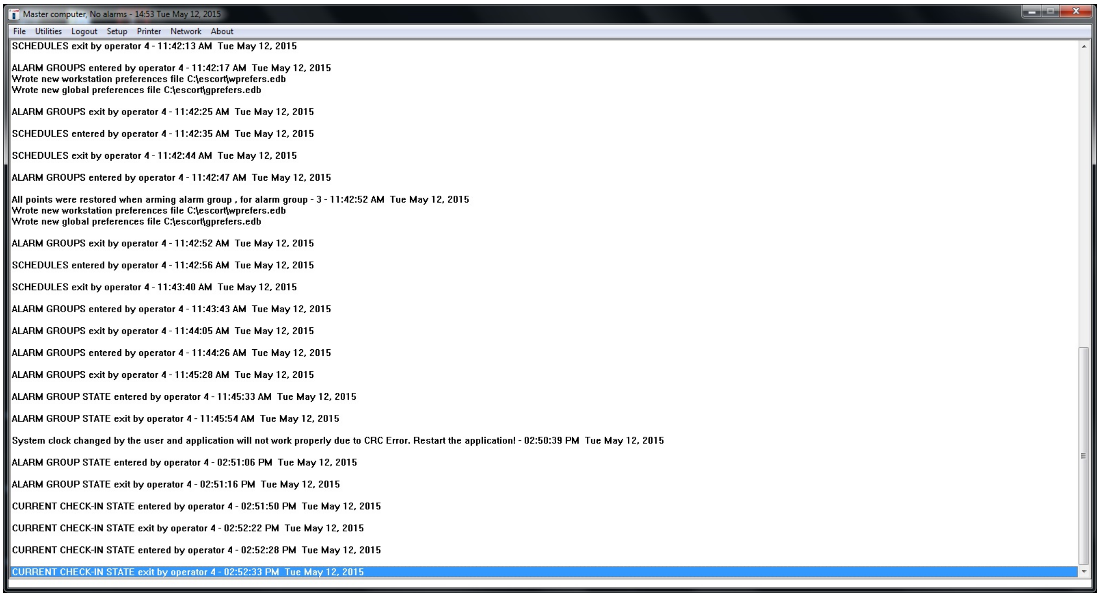
Selecting this option on the master computer causes the time on the slave and all of the workstation computers to be updated to the master computer's time.

4.3 Setup menu

4.3.1 Show history

When selected, the default map display is replaced by a scrolling text window showing the most recent events that occurred in the system. The window can list historical events and operations of the Central Console software. Examples include list of any alarms and the actions taken, name of person who logged into the Central Console, changes to the database, communication results between the devices, and so on.

The events displayed can be selected in the **History Filter** dialog under the **Setup** Menu. After **Show History** is selected, this menu item changes to **Show Map**.

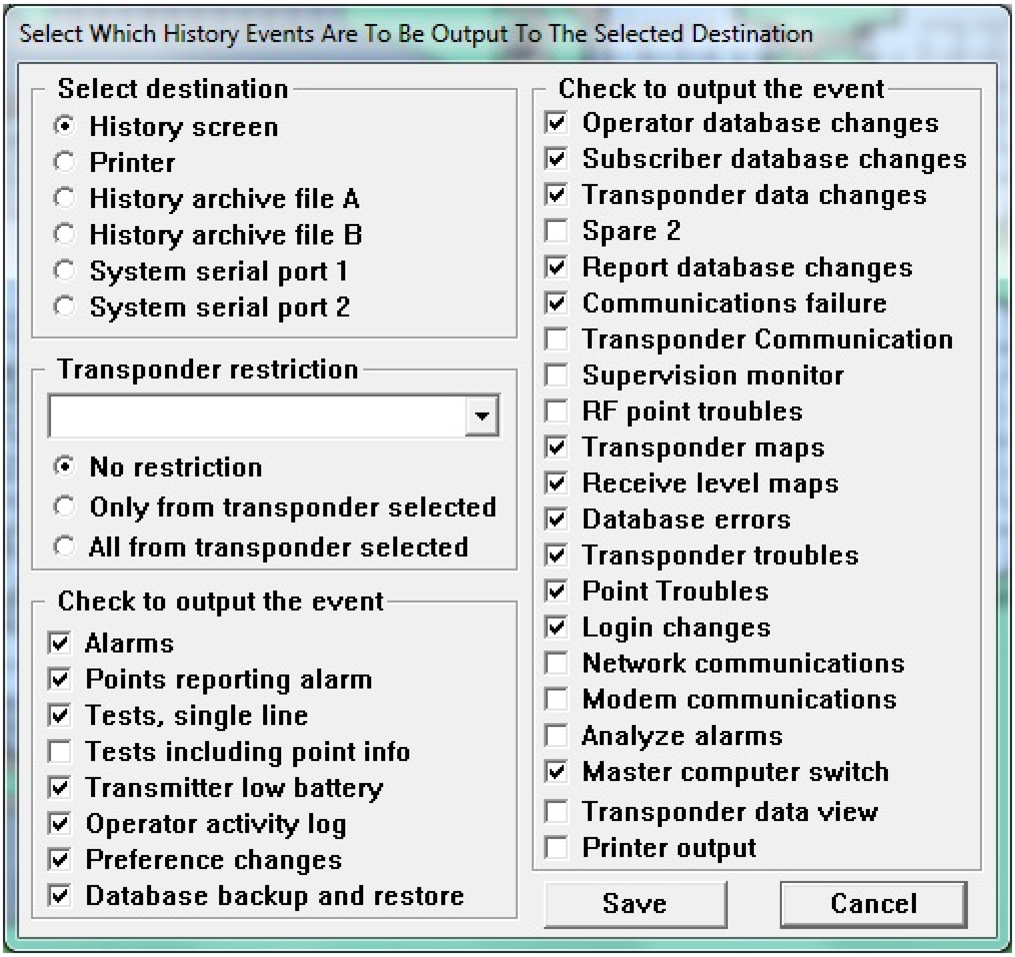

Master computer, No alarms - 14:53 Tue May 12, 2015
File Utilities Logout Setup Printer Network About

```
SCHEDULES exit by operator 4 - 11:42:13 AM  Tue May 12, 2015

ALARM GROUPS entered by operator 4 - 11:42:17 AM  Tue May 12, 2015
Wrote new workstation preferences file C:\escort\wprefers.edb
Wrote new global preferences file C:\escort\gprefers.edb

ALARM GROUPS exit by operator 4 - 11:42:25 AM  Tue May 12, 2015

SCHEDULES entered by operator 4 - 11:42:35 AM  Tue May 12, 2015

SCHEDULES exit by operator 4 - 11:42:44 AM  Tue May 12, 2015

ALARM GROUPS entered by operator 4 - 11:42:47 AM  Tue May 12, 2015

All points were restored when arming alarm group , for alarm group - 3 - 11:42:52 AM  Tue May 12, 2015
Wrote new workstation preferences file C:\escort\wprefers.edb
Wrote new global preferences file C:\escort\gprefers.edb

ALARM GROUPS exit by operator 4 - 11:42:52 AM  Tue May 12, 2015

SCHEDULES entered by operator 4 - 11:42:56 AM  Tue May 12, 2015

SCHEDULES exit by operator 4 - 11:43:40 AM  Tue May 12, 2015

ALARM GROUPS entered by operator 4 - 11:43:43 AM  Tue May 12, 2015

ALARM GROUPS exit by operator 4 - 11:44:05 AM  Tue May 12, 2015

ALARM GROUPS entered by operator 4 - 11:44:26 AM  Tue May 12, 2015

ALARM GROUPS exit by operator 4 - 11:45:28 AM  Tue May 12, 2015

ALARM GROUP STATE entered by operator 4 - 11:45:33 AM  Tue May 12, 2015

ALARM GROUP STATE exit by operator 4 - 11:45:54 AM  Tue May 12, 2015

System clock changed by the user and application will not work properly due to CRC Error. Restart the application! - 02:50:39 PM  Tue May 12, 2015

ALARM GROUP STATE entered by operator 4 - 02:51:06 PM  Tue May 12, 2015

ALARM GROUP STATE exit by operator 4 - 02:51:16 PM  Tue May 12, 2015

CURRENT CHECK-IN STATE entered by operator 4 - 02:51:50 PM  Tue May 12, 2015

CURRENT CHECK-IN STATE exit by operator 4 - 02:52:22 PM  Tue May 12, 2015

CURRENT CHECK-IN STATE entered by operator 4 - 02:52:28 PM  Tue May 12, 2015

CURRENT CHECK-IN STATE exit by operator 4 - 02:52:33 PM  Tue May 12, 2015
```

Figure 4.30: Show History Log

4.3.2 History filter dialog

This dialog selects the classes of events recorded for (sent to) specific output devices. From the **Select Destination** group, select the **History screen**, **Printer**, **History files** or **System serial ports** option. Notice that when this selection is changed, the checked items also change. There is a different set of events output for each destination selected. For each destination, the events must be individually configured.



Select Which History Events Are To Be Output To The Selected Destination

Select destination
- ● History screen
- ○ Printer
- ○ History archive file A
- ○ History archive file B
- ○ System serial port 1
- ○ System serial port 2

Transponder restriction
- ● No restriction
- ○ Only from transponder selected
- ○ All from transponder selected

Check to output the event
- ☑ Alarms
- ☑ Points reporting alarm
- ☑ Tests, single line
- □ Tests including point info
- ☑ Transmitter low battery
- ☑ Operator activity log
- ☑ Preference changes
- ☑ Database backup and restore

Check to output the event
- ☑ Operator database changes
- ☑ Subscriber database changes
- ☑ Transponder data changes
- □ Spare 2
- ☑ Report database changes
- ☑ Communications failure
- □ Transponder Communication
- □ Supervision monitor
- □ RF point troubles
- ☑ Transponder maps
- ☑ Receive level maps
- ☑ Database errors
- ☑ Transponder troubles
- ☑ Point Troubles
- ☑ Login changes
- □ Network communications
- □ Modem communications
- □ Analyze alarms
- ☑ Master computer switch
- □ Transponder data view
- □ Printer output

Figure 4.31: History Filter Dialog

History screen This option selects the events to be displayed on the computer screen when **Show History** is selected.

Printer This option selects the events to be sent to the printer.

History archive file A This option selects the events to be sent to the a_audit.txt file stored in the Security Escort sub-directory (typically C:\ESCORT \a_audit.txt). There is a minimum set of events that cannot be disabled, so they are always recorded.

History archive file B This option selects the events to be sent to the b_audit.txt file stored in the Security Escort sub-directory (typically C:\ESCORT \b_audit.txt).

System serial port 1 This option selects the events to be sent to the system serial port 1. System serial port 1 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.

System serial port 2 This option selects the events to be sent to the system serial port 2. System serial port 2 is assigned a physical comm port in the **Remote Comm Port Setup** dialog, and the **History Filter Output** field must be set in the **Remote Setup** dialog.

Transponder restriction
This option selects a transponder for the following restrictions:
No Restriction: This selection is typically left at this setting at all times. The output is not restricted by an individual transponder.
Only From Transponder Selected: The selected events are only output if they were reported from the transponder selected in the transponder above.
All from Transponder Selected : All events are reported from the transponder selected above. The selected events are reported from all other transponders in the system.

Alarms
Outputs the information about an alarm including location, but not the transponder and receiver levels. This is the data typically sent to a printer.

Points, reporting alarm
Outputs the transponder and receiver levels for an alarm. Typically, this is the data too detailed to send to a printer and is used for diagnostics, not normal system operation.

Tests, single line
Outputs the simple information about a test. Typically, this is the data normally sent to a printer.

Tests including point Info
Outputs the transponder and receiver levels for a test. This is the data usually too detailed to send to a printer and is used for diagnostics, not normal system operation. If this option is selected, **Test, single line** above, would not be selected for the same output device.

Transmitter low battery
Outputs low battery reports received from transmitters.

Operator activity log
Outputs all other operator activity (audit trail) not covered by specific event selections.

Preferences changes
Outputs all changes made to system preference selections.

Database backup and restore
Records all database backup and restore activity.

Operator database changes
Records all changes to the operator database.

Subscriber database changes
Records all changes to the subscriber database.

Transponder data changes
Records all changes to the transponder database.

Spare 2
This is a future option that has no function at this time (leave unchecked).

Report database changes
Records all changes to the **Alarm Report Database**.

Communications failure
Records all communication failures and restorations.

Transponder communication
Records all communications to transponders. This selection is only used for engineering diagnostics. Leaving this item selected generates a significant amount of history and fills up the hard disk drive quickly. Leave this item unchecked.

Supervision monitor
Reports changes in the supervision status for all transmitters that are being supervised.

RF point troubles
Output all reported radio frequency communication of receiver and alert unit troubles. Typically this item would be checked for devices used to monitor problems.

Transponder maps Outputs all transponder status maps. This selection is only used for diagnostics. Leave this item unchecked.

Receive level maps Outputs all maintenance alarm receive level maps. This selection is only used for diagnostics. Leave this item unchecked.

Database errors Outputs all reported database errors. This item is checked.

Transponder troubles Outputs all reported transponder troubles. This item is checked for devices used to monitor problems.

Point troubles Outputs all reported receiver and alert unit troubles. This item is checked for devices used to monitor problems.

Login changes Reports all new system operator login and logout activity.

Network communications Records all communications between networked computers. This selection is only used for engineering diagnostics. Leaving this item selected, generates a significant amount of history and fills up the hard disk drive very quickly and may bog down the system during high traffic times. Always leave this item unchecked.

Modem communications Records all communications to the modem for remote communications and pager access. This selection is only used for diagnosing pager communication problems. Leave this item unchecked.

Analyze alarms This option outputs data allowing an engineer to evaluate how well the location algorithm is performing. Leave this item unchecked.

Master computer switch Records when the master and slave computers switch roles.

Transponder data view Allows the data created by the **Transponder Data View** screen to be output. This selection is only used for engineering diagnostics. Leave this item unchecked.

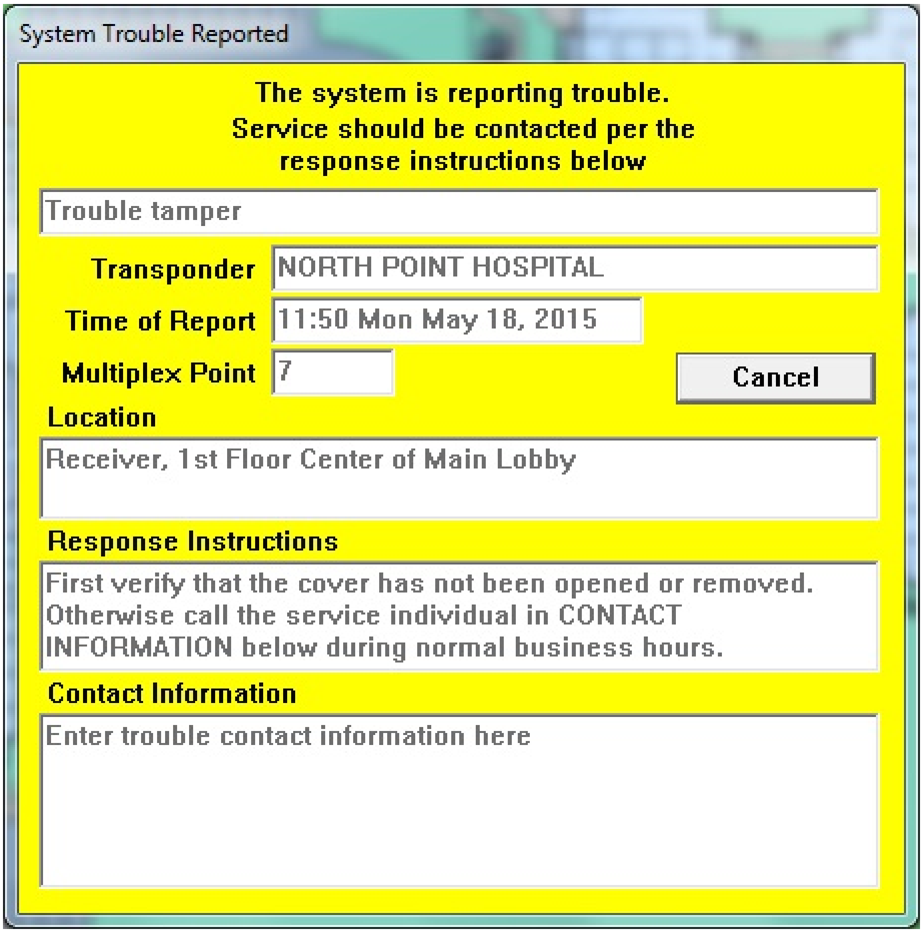
Printer output Allows the data being sent to the printer to be sent to other outputs. This item is unchecked.

4.3.3 Popup trouble filter dialog

The Security Escort System contains many built-in self testing features. Each transponder tests the condition of the receivers and alert units connected to it.

When the transponder finds a device reporting a trouble condition, it communicates the problem and the device identity to the Central Console. This generates a brief alert tone, displays a pop-up message for the operator, and sends an optional pager message. The message indicates the nature of the trouble and instructs the operator on the proper course of action. The event is recorded on the hard disks of both the main and backup computers and on the printout.

The status of the device is recorded in the **Transponder current status** dialog (See *Section Transponder current status dialog, page 69 Transponder current status dialog, page 69*) under the **Setup** menu.



System Trouble Reported

The system is reporting trouble.
Service should be contacted per the
response instructions below

Trouble tamper

Transponder: NORTH POINT HOSPITAL

Time of Report: 11:50 Mon May 18, 2015

Multiplex Point: 7

Location

Receiver, 1st Floor Center of Main Lobby

Response Instructions

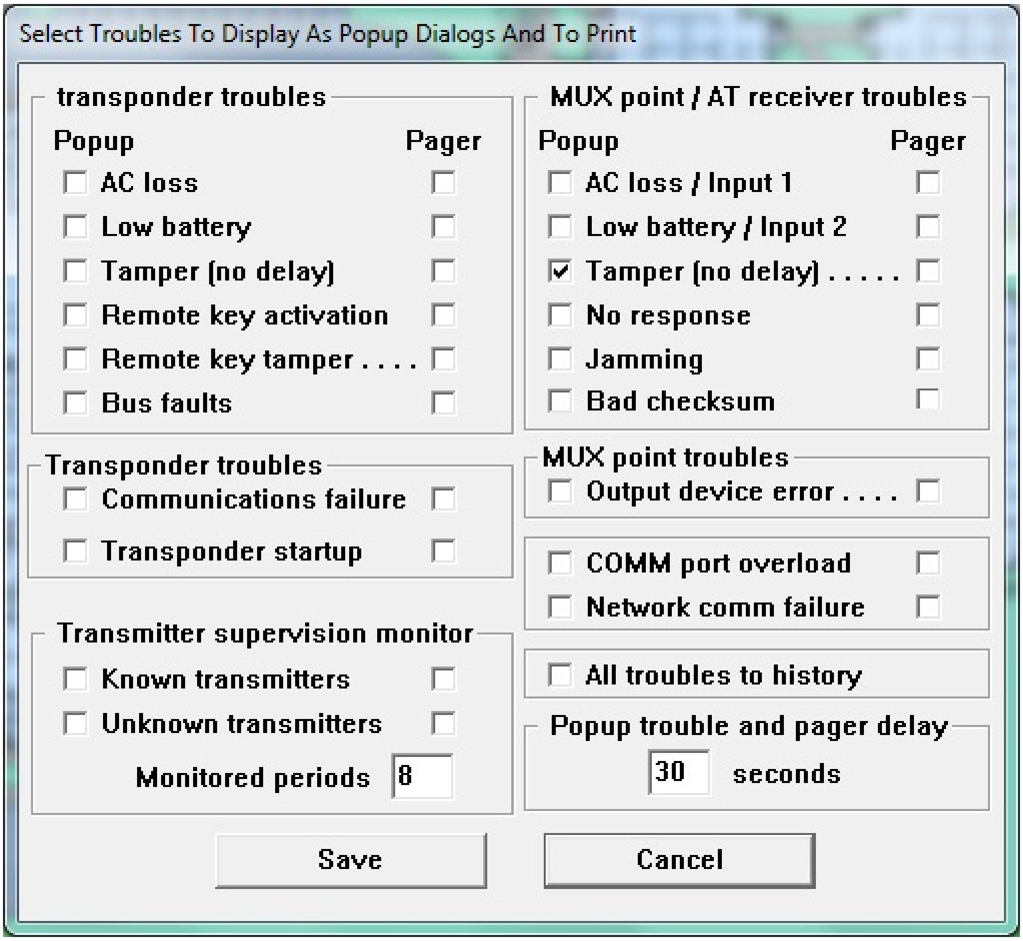
First verify that the cover has not been opened or removed. Otherwise call the service individual in CONTACT INFORMATION below during normal business hours.

Contact Information

Enter trouble contact information here

Figure 4.32: "Pop-Up" Alert Showing Tamper Trouble

This dialog allows the selection of which type of troubles that will appear in pop-up messages on the console screen, or be sent to the service pager. The troubles described below are always recorded in the **Transponder current status** window, but may or may not produce a pop-up display or pager message, depending on the selections for **Popup** or **Pager** checkboxes.



Select Troubles To Display As Popup Dialogs And To Print

transponder troubles

Popup		Pager
☐	AC loss	☐
☐	Low battery	☐
☐	Tamper (no delay)	☐
☐	Remote key activation	☐
☐	Remote key tamper	☐
☐	Bus faults	☐

MUX point / AT receiver troubles

Popup		Pager
☐	AC loss / Input 1	☐
☐	Low battery / Input 2	☐
☑	Tamper (no delay)	☐
☐	No response	☐
☐	Jamming	☐
☐	Bad checksum	☐

Transponder troubles

☐ Communications failure ☐

☐ Transponder startup ☐

MUX point troubles

☐ Output device error . . . . ☐

☐ COMM port overload ☐

☐ Network comm failure ☐

Transmitter supervision monitor

☐ Known transmitters ☐

☐ Unknown transmitters ☐

Monitored periods 8

☐ All troubles to history

Popup trouble and pager delay

30 seconds

Figure 4.33: Popup Trouble Filter Dialog

Transponder troubles group

Communications failure To continually assure that communications between the Central Console and each transponder are functioning properly, each transponder is required to send a message to the Central Console periodically. If there is no response from the transponder, the Central Console displays a communications failure warning and records the condition in the audit file.

If a transponder determines it lost communications with the Central Console, it assumes control of the outputs of the devices connected to it and transmits “I’M OK” messages until it is acknowledged by the Central Console.

Notice!

If during this loss of communications, an alarm transmission is received by one or more of the receivers attached to the transponder, the transponder activates any alert units attached to it as well as the horns and red LED’s on any of its receivers which detected the alarm transmission. Since the transponder does not have access to the **Subscriber Database**, it must assume that all transmitters are valid, so even unauthorized (not in the **Subscriber Database**) transmitters produce audible alarm indications (if the system is set for audible alarms in the **Set Security Preferences** dialog).

The Central Console also attempts to reestablish communications by continually requesting transmissions from the transponder and listening on the communications channel. When communications are restored with the Central Console, the transponder transmits any alarm and trouble conditions that occurred during the communications loss. Control of the horns, LEDs, strobes, and sirens reverts to the Central Console.

This approach to managing a communications loss assures that alarm events cannot go undetected even if the Central Console is out of operation temporarily.

AC loss

The transponder senses when it loses AC power and reports the condition to the Central Console. After a few seconds delay, the Central Console displays a pop-up alert and records the condition in the audit file. See **Transponder Current Status** dialog.

Low battery

Periodically during normal operation, the transponder tests its battery. If the test fails, it immediately reports the condition to the Central Console. After a few seconds delay, the Central Console displays a pop-up alert and the condition is recorded in the audit file.

Tamper

The transponder immediately senses and reports the actuation of its tamper switch. The Central Console immediately displays a pop-up alert and records the condition in the audit file. Tamper reports are not delayed by the pop-up trouble and pager delay.

Remote key activation

The transponder immediately senses and reports the activation (shorting) of its remote key input when it is enabled in the **Transponder Parameter** dialog. The Central Console displays a pop-up alert and records the condition in the audit file.

Remote key tamper

The transponder immediately senses and reports the fault (open) of its remote key input when it is enabled in the **Transponder Parameter** dialog. The Central Console immediately displays a pop-up alert and records the condition in the audit file.

Transponder startup

The transponder reports to the Central Console when it first starts up. This can be caused by a technician turning the transponder on or by a watchdog failure of the on board microprocessor. The Central Console immediately displays a pop-up alert and records the condition in the audit file.

Bus faults

When the transponder is unable to communicate to any receivers or alert units on one or more of its multiplex busses, it immediately reports the condition to the Central Console. The Central Console reports the condition by means of a pop-up alert if the condition persists more than a few seconds. The condition is also recorded in the audit file.

MUX bus point troubles group

AC loss
The microprocessor of the alert unit detected the absence of AC power. Loss of AC power affects only the strobe and siren functions of the alert unit. Batteries provide backup power for the strobes and sirens. The logic and communications functions derive their power from the multiplex bus.

Low Battery
The alert unit tested for a low battery condition and the test failed.

Tamper
Whenever the cover is removed from a receiver or alert unit, the on-board microprocessor detects the tamper and it is reported to the transponder. Tamper reports are not delayed by the pop-up trouble and pager delay.

No response
Whenever a receiver fails to respond to a command from the transponder, a “No Response” message is sent by the transponder to the Central Console. This can occur if a multiplex bus wire is cut or a device is damaged.

Jamming
Each receiver monitors the level of radio energy being received at all times. If the level exceeds a preset threshold, for a preset length of time, the on-board microprocessor reports jamming.

Output device error
The transponder generates this message when it commands a receiver or alert unit to activate or deactivate an output device (siren, strobe, horn, or LED) and the device fails to respond correctly.

Bad checksum
This message is generated by the transponder and sent to the Central Console whenever the transponder detects message errors in the communications between receivers and alert units.

Transmitter supervision monitoring group

Known transmitters
To continually monitor the status of all transmitters programmed in the database that send periodic supervision transmissions. If any monitored transmitters stop sending supervision transmissions, a pop-up trouble is displayed.

Unknown transmitters
To monitor for periodic supervision transmissions from transmitters not programmed in the database, a pop-up trouble displays if transmissions from transmitters not programmed in the database are received.

Monitored periods
This is the number of supervision intervals that are consecutively missed before a pop-up screen reports a specific transmitter stopped reporting supervision transmissions.

Communications port monitor

Comm port overload
A pop-up trouble screen displays if the communications traffic to the transponders exceeds the system is capability.

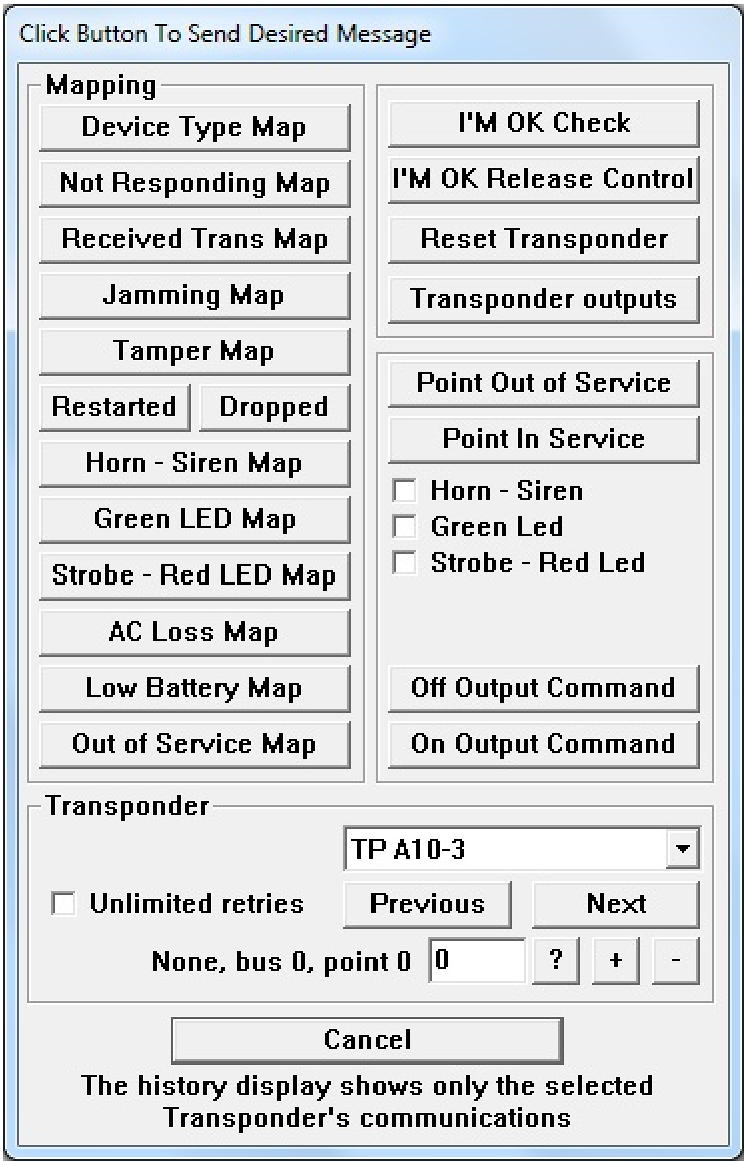
Network comm failure
A pop-up trouble screen displays if the communications between the master and slave computers fails.

Delay to ignore troubles that auto reset

Pop-up trouble and pager delay The delay in seconds before a trouble displays on the computer screen. If a restore for a trouble is received before a trouble is displayed (this delay expires), the trouble and the restore are ignored. Tamper troubles are not delayed.

4.3.4 Transponder communications dialog

From the Central Console, it is possible to perform detailed diagnostic tests using the **Transponder communications** dialog. From this dialog, the operator can request maps indicating the status of each device connected to a given transponder, and can control individual devices, turning LEDs, horns, strobes, and sirens on and off. The **Transponder communications** dialog appears on the right when it is opened, allowing the **History screen** to be viewed while the screen is open. This makes it possible to view the results of map commands issued from the console.



Transponder: TP A10-3

☐ Unlimited retries

None, bus 0, point 0: 0

The history display shows only the selected Transponder's communications

Figure 4.34: Transponder Communications dialog

Mapping commands

Diagnostic map commands are used to determine the status of all devices (connected to the selected transponder) with a single command. Maps are displayed on the **History screen** as an array of rows and columns, corresponding to point addresses and bus numbers.

The status of a particular device is shown by a “1” or “0” (zero) with “1” signifying the true state. The map location, corresponding to a device that is not responding to the transponder, contains a “1” when a **Not Responding Map** command is selected.

Similarly, a “1” is displayed in response to a **Tamper Map** command in locations that correspond to devices in a tampered state. All other locations display a “0” (zero), “a” – (if there is no device assigned to the location), or a “x”, there is a device connected to the system at that address, but it is not in the **Transponder Database**.

[Device Type Map]

Unlike all other types of map, the **Device Type Map** has two characters in each possible device location. The right most character indicates the device type. A “5” indicates a receiver, “3” indicates an alert unit, and “7” indicates that the **Transponder Database** shows a device in that location but it is not currently communicating with the transponder. The left character indicates the following: “0” (zero), the device is in its normal state, “1”, the device is off normal, and “x” there is a device connected to the system at that address, but it is not in the **Transponder Database**. (Usually this results from an error during data entry in the **Transponder Database**).

[Not Responding Map]

Requests a map of all the points that are not responding (missing) to the system on this transponder. The **[Received Transmission Map]** button produces a map display with one in the locations corresponding to receivers that are missing from the system. A “0” (zero) indicates that the point is responding. An “x” indicates there is a device connected to the system at that address, but it is not in the **Transponder Database**.

[Received Transmission Map]

As a means of self-diagnosis, the system software periodically reviews the receivers which have not received an alarm or test transmission. This list is printed as a part of the daily system status report and is a tool for assessing the health of the system. The **[Received Transmission Map]** button produces a map display with “1” in the locations corresponding to receivers which received transmissions. Each time this map is read, the **Received Transmission Map** image is cleared in the transponder.

[Jamming]

Requests a map of all the receivers that are currently reporting RF jamming to the system. The **[Jamming]** button displays a map with “1” in the locations corresponding to receivers that are reporting jamming. A “0” (zero) indicates that the receiver is not jammed.

[Tamper]

Requests a map of all the points that are currently reporting a tamper condition to the system. The **[Tamper]** button displays a map with “1” in the locations corresponding to points that are reporting tamper. A “0” (zero) indicates points that are not tampered.

[Restarted]
Requests a map of all the points that are powered up or had a watchdog failure to the system. The **[Restarted]** button displays a map with “1” in the locations corresponding to points that are restarted.

[Dropped]
Requests a map of all the receivers that have dropped one or more receptions due to high traffic. The **[Dropped]** button displays a map with “1” in the locations corresponding to receivers that dropped one or more transmissions.

[Horn - **Siren Map]**
Requests a map of all the points that have their horn or sirens on, on this transponder. The **[Horn** - **Sirens Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.

[Green LED Map]
Requests a map of all the points on this transponder that have their spare outputs - green LED on. The **[Green LED Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.

[Strobe - **Red LED Map]**
Requests a map of all the points on this transponder that have their strobe - red LED on. The **[Strobe - Red LED Map]** button displays a map with “1” in the locations corresponding to points which have their outputs on. A “0” (zero) indicates that the output is off.

[AC Loss]
Requests a map of all the alert units that are currently reporting an AC power failure to the system. The **[AC Loss]** button displays a map with “1” in the locations corresponding to alert units that are reporting AC loss.

[Low Battery Map]
Requests a map of all the alert units that are currently reporting a low battery to the system. The **[Low Battery Map]** button displays a map with “1” in the locations corresponding to points that are reporting low battery.

[Out Of Service Map]
The **Out Of Service Map** shows those points (receivers or alert units) that are currently out of service. Points may be taken out of service and returned to service by selecting the point using **MUX Bus Point** dialog in the bottom right corner of the screen and clicking the **[Point Out Of Service]** or **[Point In Service]** button. Points can be selected by typing in the point number or by using the **[+]** and **[-]** buttons, or the **[?]** button.

[I'm OK Check]
[I'm OK Release Control]

These buttons are used to diagnose and correct communications problems between the Central Console and the transponder. The system software requires that each transponder send a message to the Central Console periodically if no other communications have taken place. These messages are called "I'm OK" messages. If for some reason the communications link between the Central Console and the transponder fails, the transponder recognizes the fact when its "I'm OK" transmissions are not acknowledged by the Central Console. When the transponder has retried transmitting an "I'm OK" message or any other message six times without acknowledgment, it assumes control of the outputs (LEDs, horns, strobes, and sirens) on devices connected to it and modifies the message to indicate that it is still okay and has taken control. These messages are transmitted once per minute until communications are reestablished.

The **[I'm OK Check]** button requests that the transponder send an "I'm OK" message. This is used to determine if a transponder has taken control of its outputs. The **[I'm OK Release Control]** button generates a command to the transponder to release control back to the Central Console. Normally, the Central Console automatically generates a release control message upon the re-establishment of communications following a failure.

[Reset Transponder]

Clicking this button resets the transponder as if it was just powered up. Any test or alarm processing that was in progress at the time is lost.

[Transponder Outputs]

Requests the current state of the siren and strobe outputs on the transponder.

[Point Out Of Service]

Clicking this button takes the currently selected point out-of-service. That point no longer responds to the system, as if it was disconnected. Use this function with caution.

[Point In Service]

Clicking this button restores the currently selected point to an in-service condition. That point returns to normal function.

Horn - Siren

If this checkbox is checked, the horn output of a receiver or the siren output of an alert unit is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not checked, the state of this output is not changed.

Green LED

If this checkbox is checked, the green LED output of a receiver or the spare output of an alert unit is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not checked, the state of this output is not change.

Strobe - **Red LED** If this checkbox is checked, the red LED output of a receiver or the strobe output of an alert unit is turned on if the **[On Output Command]** button is clicked, or off if the **[Off Output Command]** button is clicked. If this checkbox is not checked, the state of this output is not changed.

[Off Output Command] When clicked, the checked horn-siren, green LED and strobe-red LED outputs are turned off for the selected point on the selected transponder. If the output does not change, click the **[On Output Command]** button and then click the **[Off Output Command]** button again.

[On Output Command] When clicked, the checked horn-siren, green LED and strobe-red LED outputs are turned on for the selected point on the selected transponder. If the output does not change, , click the **[Off Output Command]** button and then click the **[On Output Command]** button again.

Transponder Selects the transponder that you desire to communicate with.

[Previous] Returns to the previous transponder.

[Next] Advances to the next transponder.

Bus X Point Y This field displays the current bus number and point number. The actual point number may be entered in the field to the right.

[?] Opens up the **Select Point** dialog.

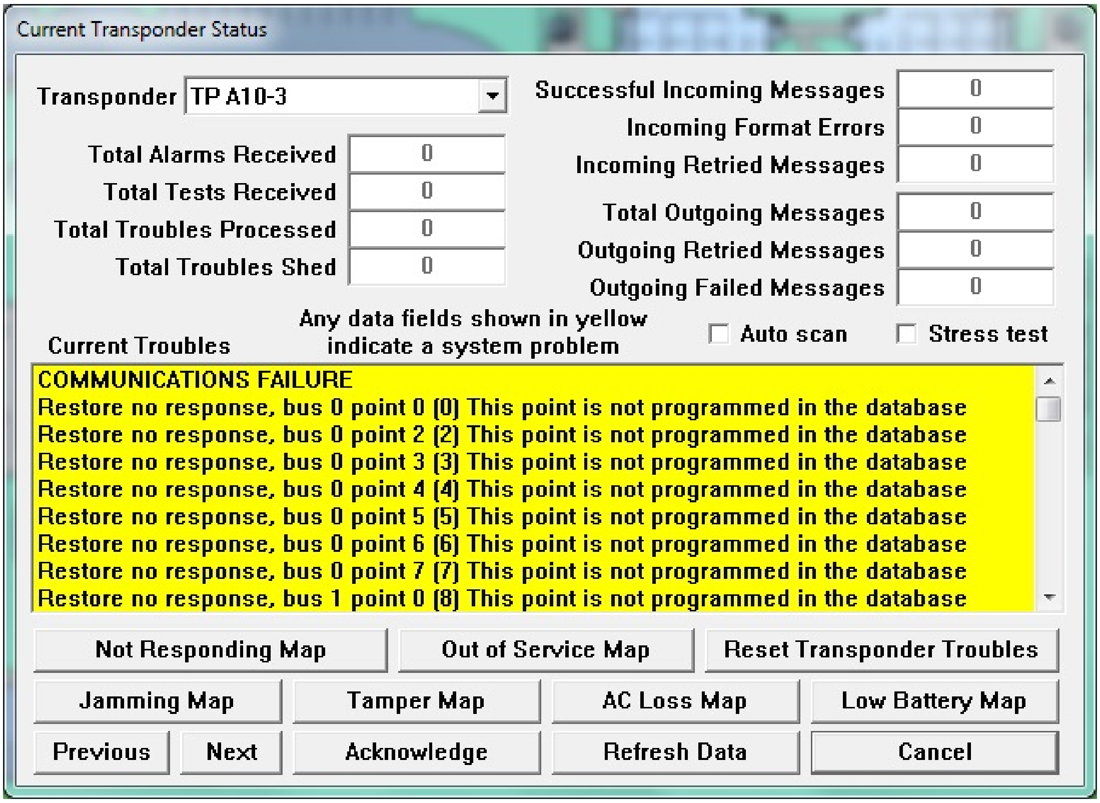
[+] Advances to the next point.

[-] Returns to the previous point.

Unlimited Retries When this checkbox is checked, the Central Console continues trying to send commands to a transponder even if the commands are not being acknowledged. (Normally, the Central Console would cease after six retries and declare a communication failure.) When this screen is closed, the system reverts to the normal six retries.

4.3.5 Transponder current status dialog

This dialog, accessible from the **main menu** under the **Setup** selection, provides a history of communications involving the transponder selected in the transponder box. It also provides several buttons that can be used to diagnose problems with the transponder and any of its receivers or alert units.


Current Transponder Status

Transponder: TP A10-3

Total Alarms Received: 0
Total Tests Received: 0
Total Troubles Processed: 0
Total Troubles Shed: 0

Successful Incoming Messages: 0
Incoming Format Errors: 0
Incoming Retried Messages: 0
Total Outgoing Messages: 0
Outgoing Retried Messages: 0
Outgoing Failed Messages: 0

Any data fields shown in yellow indicate a system problem

☐ Auto scan ☐ Stress test

Current Troubles

```
COMMUNICATIONS FAILURE
Restore no response, bus 0 point 0 (0) This point is not programmed in the database
Restore no response, bus 0 point 2 (2) This point is not programmed in the database
Restore no response, bus 0 point 3 (3) This point is not programmed in the database
Restore no response, bus 0 point 4 (4) This point is not programmed in the database
Restore no response, bus 0 point 5 (5) This point is not programmed in the database
Restore no response, bus 0 point 6 (6) This point is not programmed in the database
Restore no response, bus 0 point 7 (7) This point is not programmed in the database
Restore no response, bus 1 point 0 (8) This point is not programmed in the database
```

Figure 4.35: Transponder Current Status Screen

Transponder Selects the transponder you want to see the status of.

Total Alarms Received The total number of alarm messages received by the Central Console from this transponder since the data was last reset (using the **[Reset Transponder Troubles]** button).

Total Tests Received The total number of test messages received by the Central Console from this transponder since the data was last reset (using the **[Reset Transponder Troubles]** button).

Total Troubles Processed The total number of trouble messages received by the Central Console from the transponder and processed (see **Total Troubles Shed**) since the data was last reset (using the **[Reset Transponder Troubles]** button).

Total Troubles Shed During certain rare occurrences, the communication traffic on the transponder links becomes excessive and threatens to increase the system response time to tests and alarms. This can happen if faults are reported at a very high rate. To avoid slow response in such situations, the Central Console may go into a load shedding mode in which it ceases to record and display Trouble Reports until the communications traffic subsides. The **Total Troubles Shed** box indicates the number of trouble messages that were not processed since the last reset (using **[Reset Transponder Troubles]** button).

Successful Incoming Messages The total number of messages successfully received from this transponder.

Incoming Format Errors
The number of messages received from this transponder where format error was detected. This field is yellow if 1.5% or more of the messages had errors. A high level of message errors indicates a serious communication problem.

Incoming Retried Messages
The total number of messages successfully received from this transponder that indicated they were retried. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.

Total Outgoing Messages
The total number of messages sent to this transponder from the Central Console.

Outgoing Retried Messages
The total number of message retries to this transponder. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.

Outgoing Failed Messages
This is total number of messages that could not to be delivered to this transponder. This field is yellow if there are any failed messages. Outgoing failed messages cause the Central Console to display an alert message that communications have failed.

Auto scan
The auto scan function performs the above stress test proceeding from one transponder to the next after one of each type of map is requested and received. After the last map type and before proceeding to the next transponder, a command is issued to refresh the transponder data so that when an auto scan proceeds through all transponders, all transponder and point troubles are updated. Auto scan is terminated by removing the check in the **Auto scan** checkbox or by closing the screen using the **[Cancel]** button.

Stress test
This checkbox causes the Central Console to continually request maps from the transponder. When in this mode, the Central Console sends a new map request as soon as it receives a map from the transponder, rotating through the map types. This test is used when diagnosing communications problems to create artificially high traffic on the communication link without interfering with the processing of alarms and tests. The stress test ceases when the checkbox is cleared, or this screen is closed by clicking the **[Cancel]** button.

Current Troubles
This window displays all current troubles for this transponder. In the **Current Transponder Status** dialog, there is a low battery and a tamper condition being reported for this transponder. This window also displays the restoration to a normal condition when it occurs. When the fault is corrected, clicking the **[Acknowledge]** button eliminates any restoration reports. Conditions, which were not rectified, remain in the window.

[Not Responding Map] To assist in diagnosing problems with the receivers and alert units associated with a transponder, several commands can be issued from the Central Console to requesting information from the transponder. This button requests a map of all the devices on this transponder (receivers or alert units) that are not responding to the system. The current troubles list is automatically updated.

[Out of Service Map] This button requests a map of all devices on this transponder (receivers or alert units) that were manually taken out of service to the system. The current troubles list is automatically updated.

[Reset Transponder Troubles] This button is used to reset all of the alarm, test and message counters to zero, and to remove any restoration reports.

[Jamming Map] This button requests a map of all the receivers on this transponder that are reporting a jamming condition to the system. The **Current Troubles** list is automatically updated.

[Tamper Map] This button requests a map of all the devices on this transponder (receivers or alert units) that are reporting a tamper condition to the system. The current troubles list is automatically updated.

[AC Loss Map] This button requests a map of all the alert units on this transponder that are reporting an AC loss condition to the system. The current troubles list is automatically updated.

[Low Battery Map] This button requests a map of all the alert units on this transponder that are reporting a low battery condition to the system. The current troubles list is automatically updated.

[Previous] Returns to the previous transponder.

[Next] Advances to the next transponder.

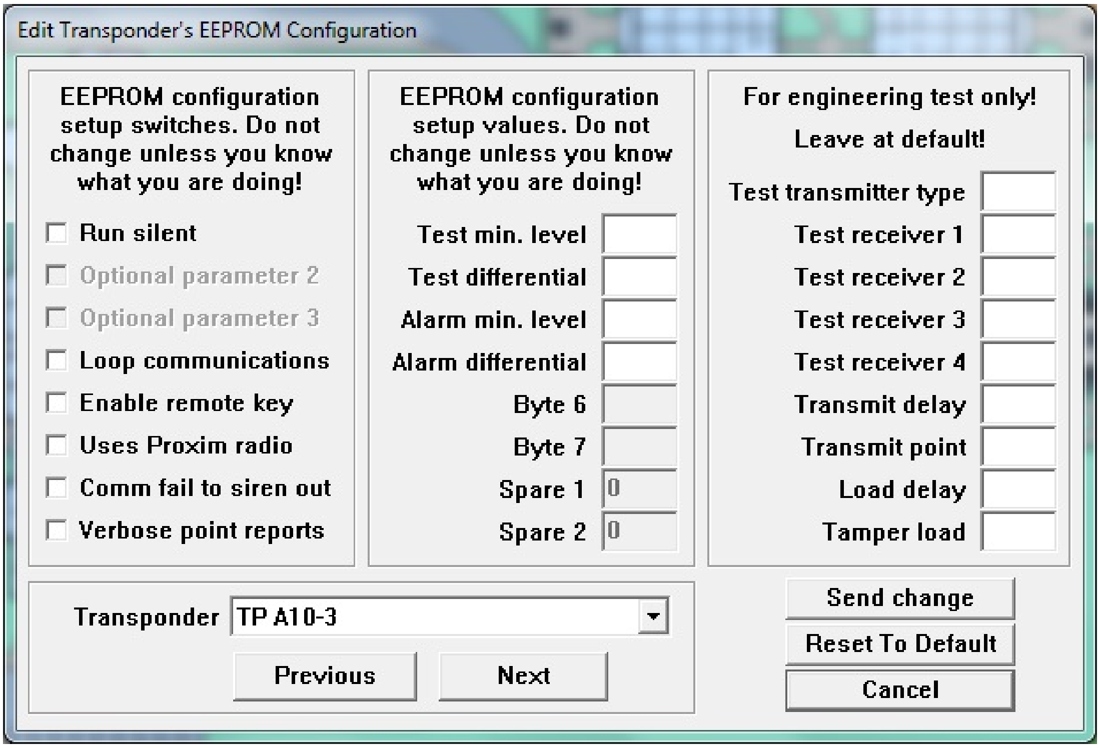
[Acknowledge] Clicking this button removes all restored troubles from the current troubles list.

[Refresh Data] Clicking this button updates all of the transponder level data in this screen. It does not update the device troubles (use stress test or auto scan to update the device troubles).

[Cancel] Clicking this button cancels all commands and close the dialog window..

4.3.6 Transponder parameter change dialog

This dialog allows parameters stored in the transponder’s EEPROM memory to be viewed and changed.



Edit Transponder's EEPROM Configuration

EEPROM configuration setup switches. Do not change unless you know what you are doing!

- □ Run silent
- □ Optional parameter 2
- □ Optional parameter 3
- □ Loop communications
- □ Enable remote key
- □ Uses Proxim radio
- □ Comm fail to siren out
- □ Verbose point reports

EEPROM configuration setup values. Do not change unless you know what you are doing!

Test min. level	
Test differential	
Alarm min. level	
Alarm differential	
Byte 6	
Byte 7	
Spare 1	0
Spare 2	0

For engineering test only!

Leave at default!

Test transmitter type	
Test receiver 1	
Test receiver 2	
Test receiver 3	
Test receiver 4	
Transmit delay	
Transmit point	
Load delay	
Tamper load	

Transponder: TP A10-3

Figure 4.36: Transponder Parameter Change Dialog

Run silent If checked, the receivers and alert units on this transponder do not sound an alarm. This includes alarms received during a communications failure with the Central Console.

Optional parameter This option is currently disabled and reserved for future use.

Loop communications Normally the transponders are connected in parallel (party line) so they can all hear if any other transponders are in communications so they don't collide when communicating. However if fiber optic communications is used between the transponders and PC they can't be connected this way. Therefore they are connected in a loop. The transmission from the PC goes to the receiver on the first transponder. The transmission from the first transponder goes to the receiver on the second transponder and so on, until the transmission from the last transponder goes to the receiver on the PC. This option tells the transponders they are connected this way so it can react. You must make this change to the first transponder first, followed with the second, continuing in order until all is done.

Enable remote key(If checked, the remote key supervised input on this transponder is enabled. Otherwise it will be ignored.

Uses Proxim radio Only check this item if a Proxim radio is used to communicate to the Central Console.

Comm fail to siren out If this item is checked, the siren output on this transponder activates when a communications failure is detected at the Central Console.

Verbose point reports If checked, alarm and test reports include average levels and packet count information. This extra information is for diagnostic proposes only and is not required for system operation. Since the additional data increases the system traffic load leave this item unchecked.

Test min level This is the minimum receive level (1 to 255) a receiver must see before the green light displays acknowledging a successful test. Leave this item at default (128).

Test differential This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing a test before the green light displays acknowledging a successful test. Leave this item at default (64).

Alarm min level This is the minimum receive level (1 to 255) a receiver must see before the sounder and red light is displayed for an alarm. Leave this item at default (1).

Alarm differential This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing an alarm before the sounder and red light are displayed for an alarm. Leave this item at default (255).

Byte These are future options, leave at default (0).

Spare These are future options, leave unchecked..

Test transmitter type
Test receiver 1, 2, 3, 4
Transmit delay
Transmit point
Load delay
Tamper load

These parameters are used for engineering system load testing only. **Do not use in a live system**, as they can generate more traffic than a system can handle; therefore, actual alarms may be missed. Leave them at default.

Transponder Selects the transponder the data is presented for.

[Previous] Returns to the previous transponder in the system.

[Next] Advances to the next transponder in the system.

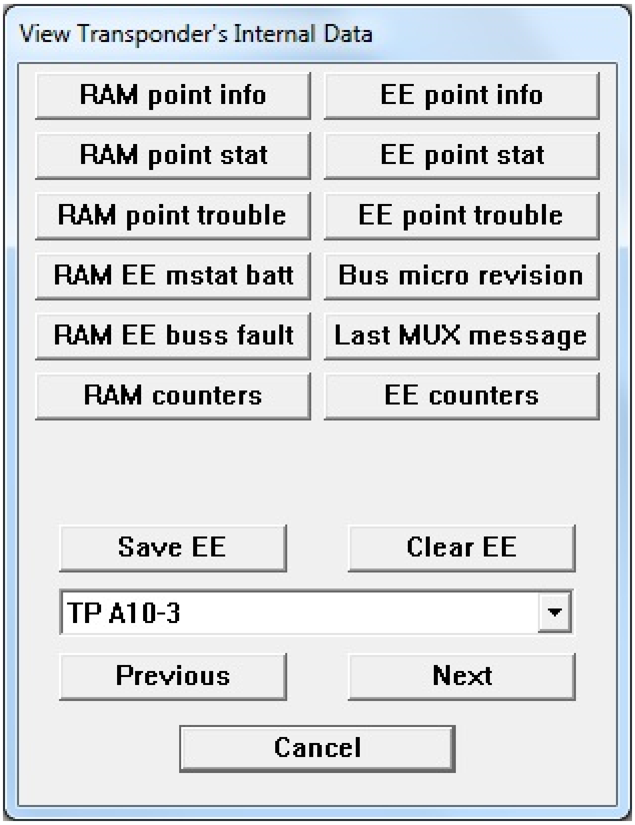
[Send change] Sends the changes made to the selected transponder. Changes are not made to the transponder EEPROM memory unless this button is clicked.

[Reset to Default] Reset the selected transponder to the default settings.

[Cancel] Cancel the operation and close the dialog window.

4.3.7 Transponder data view dialog

This dialog is solely for engineering evaluation of the transponder only.



TP A10-3

Figure 4.37: Transponder Data View Dialog

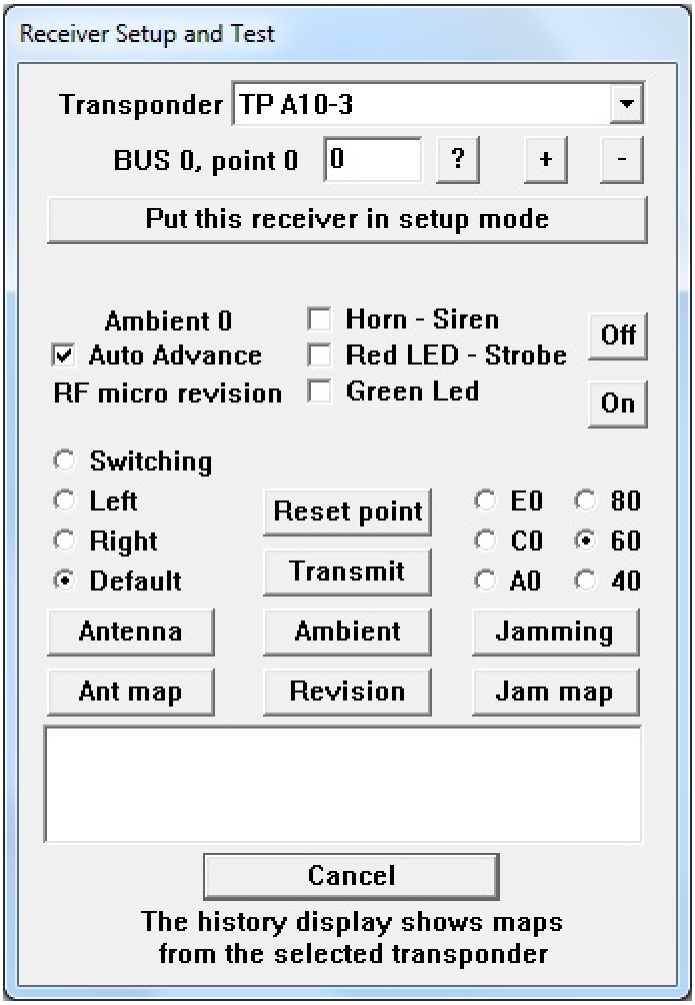
[RAM point info]	Views the RAM image of point information.
[RAM point stat]	Views the RAM image of point status.
[RAM point trouble]	Views the RAM image of point trouble.
[RAM EE mstat batt]	Views the RAM and EEPROM images of transponder status and battery condition.
[RAM EE buss fault]	Views the RAM and EEPROM images of transponder MUX bus fault condition.
[RAM counters]	Views the RAM image of the process registers.
[EE point info]	Views the EEPROM image of point information.
[EE point stat]	Views the EEPROM image of point status.
[EE point trouble]	Views the EEPROM image of point trouble.
[Bus micro revision]	Views the bus micro revision for the connected points.
[Last MUX message]	Views the last MUX bus message received.
[EE counters]	Views the EEPROM image of the process registers.
[Save EE]	Saves the current RAM image to the EEPROM memory on the transponder.
[Clear EE]	Clears the EEPROM memory on the transponder and resets the transponder.
[Previous]	Returns to the previous transponder in the system.

[Next] Advances to the next transponder in the system.

[Cancel] Cancels the operation and closes the dialog window.

4.3.8 Receiver configuration dialog

Once the receiver and alert unit data for a transponder has been entered into the **Transponder Database**, this dialog is used to verify that each receiver is working and is properly addressed in the database. This setup tool identifies errors in the address switch settings of receivers and alert units as well as data entry errors in the **Transponder Database**.



Receiver Setup and Test

Transponder: TP A10-3

BUS 0, point 0: 0

Ambient 0

☑ Auto Advance

RF micro revision

□ Horn - Siren

□ Red LED - Strobe

□ Green Led

○ Switching

○ Left

○ Right

● Default

○ E0 ○ 80

○ C0 ● 60

○ A0 ○ 40

The history display shows maps from the selected transponder

Figure 4.38: Receiver Configuration Dialog

[Put this receiver in setup mode] This button initiates the setup process by causing both the red and green LED of the selected receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes the **[Abort setup for this MUX Point]** button to be able to proceed to the next device in the event that one receiver is not set up properly.

Ambient value The **Ambient** value, shown above **Auto Advance,** shows the current ambient level at the receiver. To get an updated ambient reading, select the point and click the **[Transmit]** button followed by the **[Ambient]** button.

Auto Advance

If this checkbox is checked, the Central Console automatically selects the receiver with the next higher point address.

RF micro revision

The receiver’s RF micro revision level is shown below **Auto Advance**. To get an updated reading, click the **[Revision]** button.

Horn - Siren

If this checkbox is checked, the horn output of a receiver or the siren output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.

Red LED - Strobe

If this checkbox is checked, the red LED output of a receiver or the strobe output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.

Green Led

If this checkbox is checked, the green LED output of a receiver or the spare output of an alert unit is turned on upon clicking the **[On]** button, or turned off upon clicking the **[Off]** button. If this checkbox is not checked, the state of this output does not change.

[Off]

Upon clicking the button, any checked outputs (**Horn-Siren**, **Green LED**, **Red LED - Strobe**) is turned off for the selected point on the selected transponder. If the output does not change, click the **[On]** button followed by the **[Off]** button again.

[On]

Upon clicking the button, any checked outputs (**Horn-Siren**, **Green LED**, **Red LED - Strobe**) is turned on for the selected point on the selected transponder. If the output does not change, click the **[Off]** button followed by the **[On]** button again.

[Antenna]

Normally, a receiver automatically switches between its diversity antennas during normal operation (leave the default selection on a working system at this setting). The receiver can be forced to use only the left or right antenna, or always switch by selecting the appropriate setting and clicking the **[Antenna]** button.

[Ant map]

Clicking the **[Ant map]** button causes the system to interrogate the current antenna switching settings of all receivers on this transponder.

[Reset point]

Clicking the **[Reset point]** causes the microprocessors on this point to reset as if they were just powered up. A receiver should not be reset in a working system, as it can cause receptions to be lost.

[Transmit]

Clicking the **[Transmit]** button causes this receiver to send one test transmission.

[Ambient] Clicking the **[Ambient]** button causes the system to interrogate the current ambient levels of all receivers on this transponder.

[Revision] Clicking the **[Revision]** button causes the system to interrogate the RF micro revision levels of all receivers on this transponder.

[Jamming] A receiver monitors the ambient level during normal operation. If the ambient level rises above the jamming setting and jamming trouble, it is reported to the Central Console. The receiver’s jamming level can be adjusted by selecting the appropriate setting (shown in hexadecimal levels) and clicking the **[Jamming]** button.

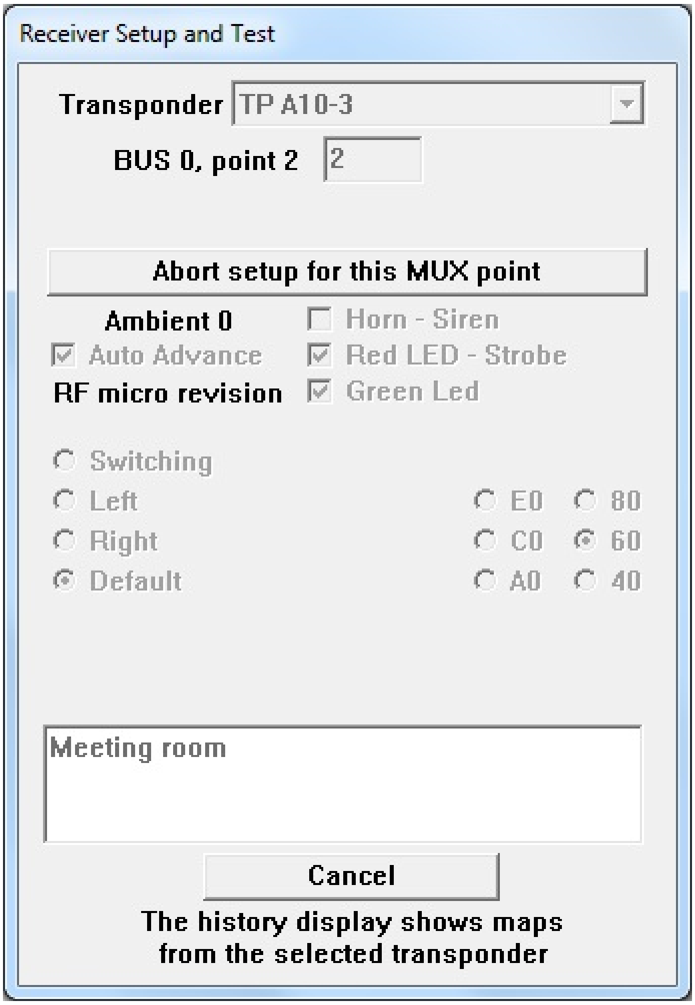
[Jam map] Clicking the **[Jam map]** button causes the system to interrogate the jamming setting levels of all receivers on this transponder.

[Cancel] Clicking the **[Cancel]** button closes the dialog window.

Put this receiver in setup mode
This button initiates the setup process by causing both the red and green LED of the selected receiver to light up. The red and green LED will be flashing. On the Central Console, this button changes the **[Abort setup for this MUX point]** button to be able to proceed to the next device in the event that one receiver is not set up properly.
The next step is using a maintenance transmitter to transmit an alarm while standing near the receiver.

Notice!
The illuminated LED indicate to the service person standing near the device that the receiver is actually the one currently in the setup mode. If the LED of the designated receiver are not illuminated, there is probably an error in the switch settings of the receiver or an error in the address in the **Transponder Database**. To help resolve such problems, the person at the Central Console can command any device to illuminate its LED and/or sound its horn.

If the receiver in the setup mode detects the maintenance alarm and if the received signal is the strongest of all receivers, the horn on the receiver sounds briefly and the LEDs go off. This indicates the receiver is functioning properly and the receiver’s address is set correctly in the **Transponder Database** and on the receiver’s switches.



Receiver Setup and Test

Transponder: TP A10-3

BUS 0, point 2: 2

Ambient 0

☑ Auto Advance

RF micro revision

☐ Horn - Siren

☑ Red LED - Strobe

☑ Green Led

○ Switching
○ Left
○ Right
● Default

○ E0 ○ 80
○ C0 ● 60
○ A0 ○ 40

Meeting room

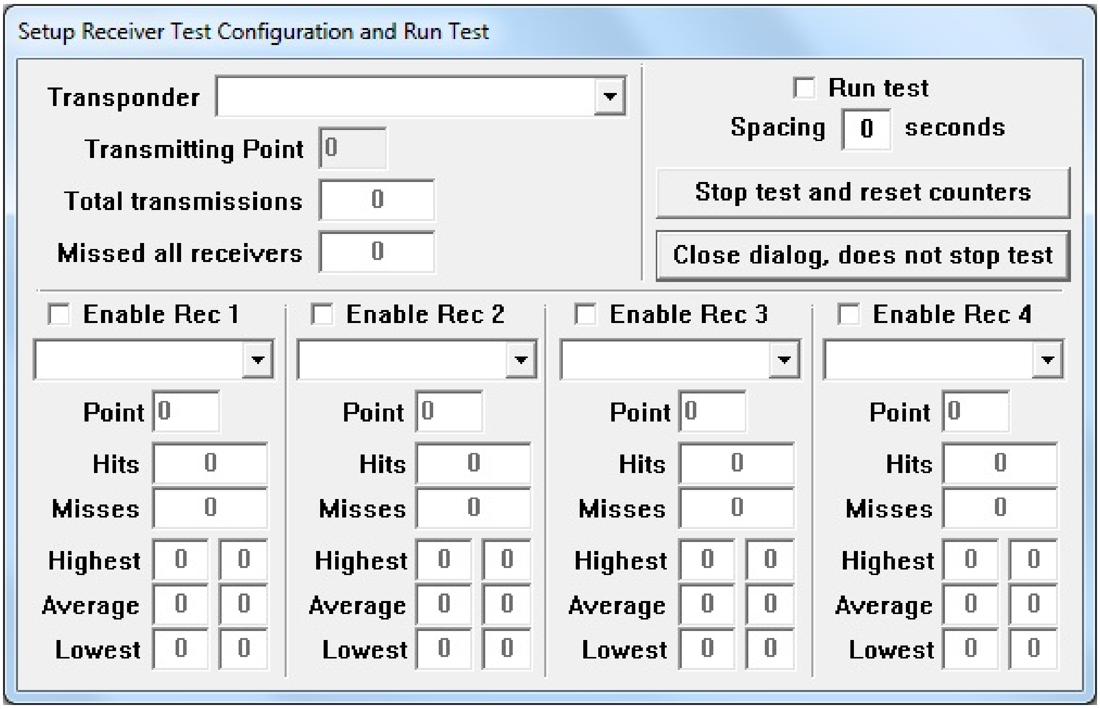
The history display shows maps from the selected transponder

Figure 4.39: Abort Button to Remove a Device from the Setup Mode

The Central Console also confirms the successful setup with an audible and text message. The **[Abort setup for this MUX point]** button disappears and is replaced by **[Test on this MUX point SUCCESSFUL]** button. Click this button to conclude the test on this point.

4.3.9 Receiver test dialog

Use this dialog to set up and monitor four receivers, and listen to one receiver transmitting with its buddy check transmitter. Normally, the function is for engineering evaluation of new transmitter and receiver designs, but it can be used to test receiver boards and locations in a working system.



Setup Receiver Test Configuration and Run Test

Transponder

Transmitting Point 0

Total transmissions 0

Missed all receivers 0

□ Run test

Spacing 0 seconds

Stop test and reset counters
Close dialog, does not stop test

□ Enable Rec 1			□ Enable Rec 2			□ Enable Rec 3			□ Enable Rec 4		
Point	0		Point	0		Point	0		Point	0	
Hits	0		Hits	0		Hits	0		Hits	0	
Misses	0		Misses	0		Misses	0		Misses	0	
Highest	0	0	Highest	0	0	Highest	0	0	Highest	0	0
Average	0	0	Average	0	0	Average	0	0	Average	0	0
Lowest	0	0	Lowest	0	0	Lowest	0	0	Lowest	0	0

Figure 4.40: Receiver Test Dialog

Transponder
Select the transponder for the transmitting point and each receiving point. They can be on the same or different transponders.

Transmitting Point
Select the point (receiver) on the selected transponder to generate the transmissions.

Total transmissions
The total number of times the designated receiver transmitted the test message.

Missed all receivers
The total number of times where the test transmission was not heard by any of the designated receivers.

Enable Rec
This checkbox must be checked for this receiver to monitor the test transmissions.

Point
Select the point (receiver) on this transponder to monitor the test transmissions.

Hits
The number of times this receiver successfully heard the test transmission.

Misses
The number of times this receiver failed to hear the test transmission.

Highest
The left box displays the highest receive level at which the test transmission was heard. The right box displays the greatest number of packets heard from a single test transmission.

Average
The left box displays the average receive level at which the test transmission was heard. The right box displays the average number of packets heard from a single test transmission.

Lowest The left box displays the lowest receive level at which the test transmission was heard. The right box displays the least number of packets heard from a single test transmission.

Run test The test only runs when this checkbox is checked. To stop the test and retain the test values, uncheck this checkbox.

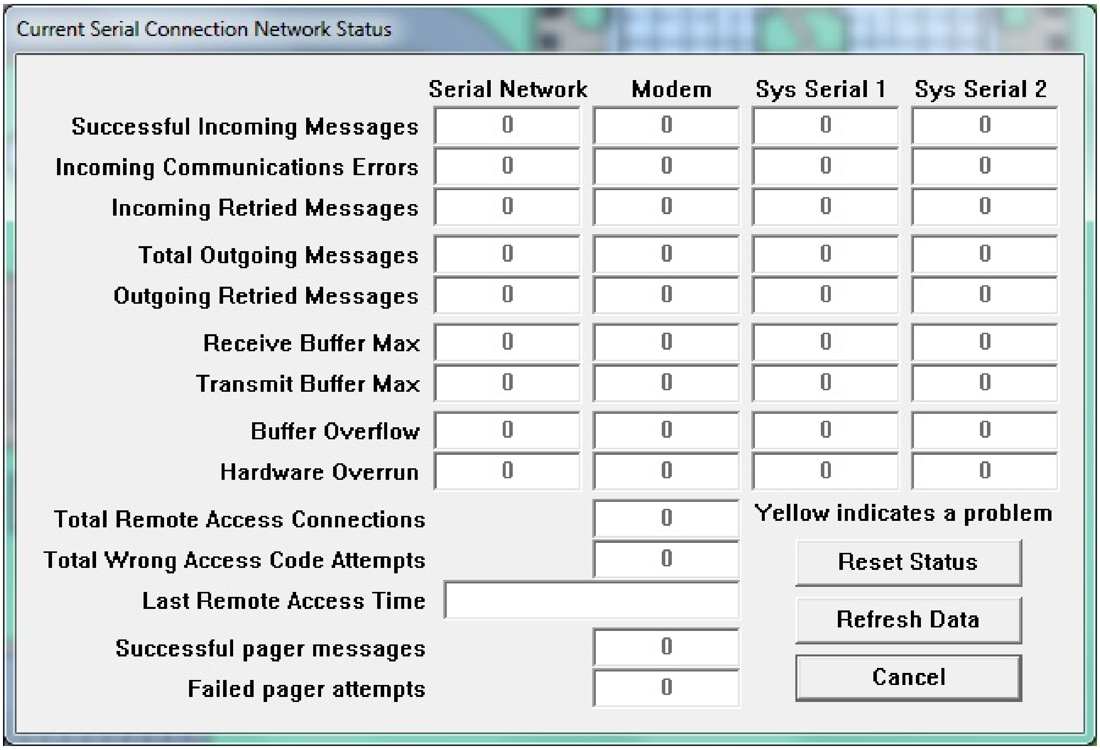
Spacing This slows the test by forcing this number of seconds between test transmissions. Normally, this setting is left at the default of 0.

Stop test and reset counters Clicking this button stops the test and resets all values.

Close dialog, does not stop test Clicking this button closes this dialog but does not stop the test from running. Reopening the dialog displays the current progress of the test. The test should not be left running unless there is a specific need, as it generates both RF and system traffic.

4.3.10 Network status dialog

This dialog shows the status of communications on the network, modem, and system serial ports.



Current Serial Connection Network Status

	Serial Network	Modem	Sys Serial 1	Sys Serial 2
Successful Incoming Messages	0	0	0	0
Incoming Communications Errors	0	0	0	0
Incoming Retried Messages	0	0	0	0
Total Outgoing Messages	0	0	0	0
Outgoing Retried Messages	0	0	0	0
Receive Buffer Max	0	0	0	0
Transmit Buffer Max	0	0	0	0
Buffer Overflow	0	0	0	0
Hardware Overrun	0	0	0	0

Total Remote Access Connections	0
Total Wrong Access Code Attempts	0
Last Remote Access Time	
Successful pager messages	0
Failed pager attempts	0

Figure 4.41: Network Status Dialog

Successful Incoming Messages This value is the number of messages that the system successfully received on this communication port.

Incoming Communication Errors This value is the number of messages that the system detected errors in, on this communication port. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.

Incoming Retried Messages This value is number of successful receptions that indicated that they retried by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.

Total Outgoing Messages This value is total number of outgoing messages sent on this port.

Outgoing Retried Messages This value is number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.

Receiver Buffer Max This value is maximum number of bytes received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

Transmit Buffer Max This value is maximum number of bytes processed by the system, but not yet transmitted on this serial port. If displayed in yellow, more than 50% of the queue was in use.

Buffer Overflow This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.

Hardware Overrun This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.

Total Remote Access Connections This value is the total number of times a remote access connection was successful.

Total Wrong Access Code Attempts This value is the number of times a remote access connection was attempted and rejected because a valid remote access code was not received.

Last Remote Access Time This is the time and date of the last successful remote access attempt.

Successful pager messages This value is the number of successful pager messages sent.

Failed pager attempts This value is the number of times a pager message dial-out was unsuccessful.

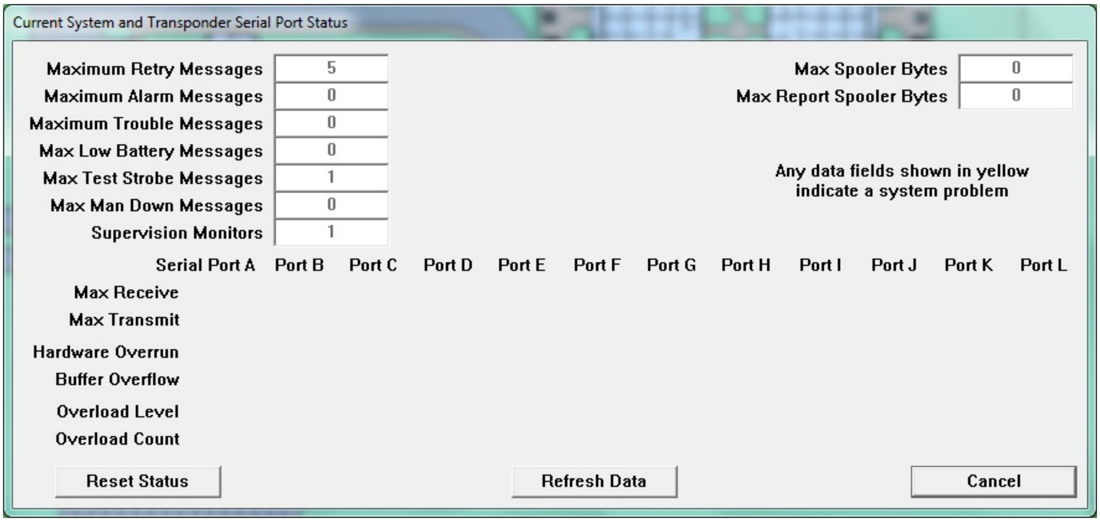
[Reset Status] Clicking this button resets all values shown in this dialog.

[Refresh Data] Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.

[Cancel] Clicking this button closes the dialog window.

4.3.11 System status dialog

This dialog shows the status of internal system queues and communications on the serial ports assigned to transponders.



Current System and Transponder Serial Port Status

Maximum Retry Messages 5
Maximum Alarm Messages 0
Maximum Trouble Messages 0
Max Low Battery Messages 0
Max Test Strobe Messages 1
Max Man Down Messages 0
Supervision Monitors 1

Max Spooler Bytes 0
Max Report Spooler Bytes 0

Any data fields shown in yellow indicate a system problem

Figure 4.42: System Status Dialog

Maximum Retry Messages This value is maximum number of messages in queue to be sent to all transponders in the system, and were not yet acknowledged. If displayed in yellow, more than 50% of the queue was in use at this value.

Maximum Alarm Messages This value is the maximum number of alarms that the system processed at its busiest time. If displayed in yellow, more than 50% of the maximum was in use.

Maximum Trouble Messages This value is the maximum number of troubles in the queue yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Max Low Battery Messages This value is the maximum number of transmitters with low batteries yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Max Test Strobe Messages This value is the maximum number of test strobes in use at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Man Down Messages This value is the maximum number of transmitters timing man down events, at one time. If displayed in yellow, more than 50% of the queue was in use.

Supervision Monitors This value is the current number of transmitters being monitored for supervision transmissions.

Max Spooler Bytes This value is the maximum number of bytes spooled for the printer at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Report Spooler Bytes This value is the maximum number of bytes spooled for the printer for Guard Tour Reports at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Receiver Buffer This value is the maximum number of bytes received from transponders on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

Max Transmit Buffer This value is the maximum number of bytes processed by the system, but not yet transmitted to the transponders on this serial port. If displayed in yellow, more than 50% of the queue was in use.

Hardware Overrun This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.

Buffer Overflow Count This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.

Overload Level This is a measure of the amount of time peak traffic on this serial port was greater than the system’s ability to handle it. The system automatically sheds non-essential tasks when this value rises.

Overload Count This is a measure of the number of times peak traffic on this serial port was greater than the system’s ability to handle it. The system automatically sheds non-essential tasks when this value rises.

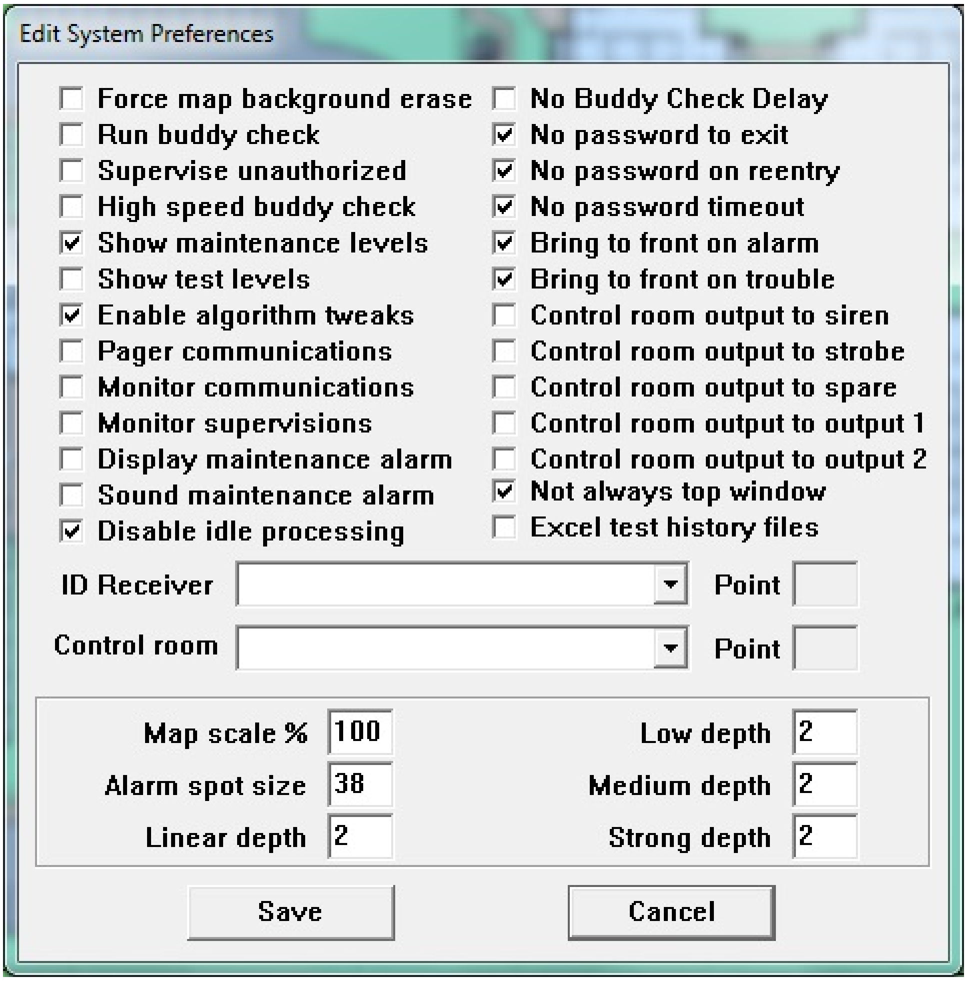
[Reset Status] Clicking this button resets all values in this shown in this dialog.

[Refresh Data] Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.

[Cancel] Clicking this button closes the dialog window.

4.3.12 System preferences dialog

The **System preferences** dialog under the **Setup** menu contains a number of settings that govern the behavior of the Security Escort System.



Edit System Preferences

☐ Force map background erase
☐ Run buddy check
☐ Supervise unauthorized
☐ High speed buddy check
☑ Show maintenance levels
☐ Show test levels
☑ Enable algorithm tweaks
☐ Pager communications
☐ Monitor communications
☐ Monitor supervisions
☐ Display maintenance alarm
☐ Sound maintenance alarm
☑ Disable idle processing

☐ No Buddy Check Delay
☑ No password to exit
☑ No password on reentry
☑ No password timeout
☑ Bring to front on alarm
☑ Bring to front on trouble
☐ Control room output to siren
☐ Control room output to strobe
☐ Control room output to spare
☐ Control room output to output 1
☐ Control room output to output 2
☑ Not always top window
☐ Excel test history files

ID Receiver: Point:

Control room: Point:

Map scale %: 100
Alarm spot size: 38
Linear depth: 2
Low depth: 2
Medium depth: 2
Strong depth: 2

Figure 4.43: System Preferences Dialog

Force map background erase Use this checkbox to erase the map screen. It should only be checked if there are problems with icons not being cleared properly from the screen. Otherwise it will cause the screen to flicker.

Run buddy check This checkbox enables and disables the buddy check feature of the system. When checked, the Central Console periodically issues a command (via the transponders) to each receiver, to activate its on-board transmitter. The Central Console then compares the signals received from neighboring receivers to the results of earlier buddy checks, thus identifying receivers, which appear to have changed sensitivity.

Day month format Checking this checkbox causes all dates to be presented in day month year format rather than the month day year format used in North America.

Supervise unauthorizedt Supervise unauthorized transmitter.

High speed buddy check Checking this checkbox allows the buddy check to run as fast as it can. Normally, only one buddy check transmission is sent each minute.

Show maintenance levels Checking this checkbox causes the Central Console to display the signal strength measured by each receiver as a number (from 1 to 15) inside the receiver icon when maintenance alarms are displayed. Otherwise, the floor number is displayed.

Show test levels Checking this checkbox causes signal strength levels to appear on the receiver icons when displaying tests on the main map screen. Otherwise the green test” icons are displayed.

Enable algorithm tweaks Checking this checkbox causes the Map Scale, Alarm Spot Size, and depth settings to be displayed in this dialog. It also controls the display of the **SA%** and **Algorithm** settings in the **Edit Transponder's Database Record** dialog

Pager communications Normally, this checkbox is not checked. If checked, the communications to the dial-up wide area paging system through the modem will be displayed on the history screen. This function is only used to diagnose communications problems to the paging system.

Monitor communications Normally, this checkbox is not checked. If checked, the communications to the modem will be displayed on the history screen. This function is only used to diagnose communications problems with the modem.

Monitor supervisions Monitor supervision alarms.

Display maintenance alarm Normally, when a maintenance alarm is received from a maintenance transmitter, the red LED on all receivers hearing the transmission will flash for 5 seconds. If this checkbox is checked, the receiver with the loudest reception level will turn on both the red and green LED for 5 seconds.

Sound maintenance alarm If this checkbox is checked, the receiver with the loudest reception level on a maintenance alarm will turn on its sounder for 5 seconds. Normally this checkbox is not checked.

Disable idle processing Normally this software registers with Windows to return to the Security Escort System if there is any idle time. The Security Escort System can use it to speed up its response to serial communications and other background tasks. If checked, the software will not register for the idle time. Normally, this checkbox is not checked. Windows can show the amount of time each application (task) is taking. When this checkbox is not checked, it may appear that Security Escort System is “hogging” the processor resources. This is not true, because the Security Escort System is only taking the time that Windows gives it through the idle process. To prove this, check this checkbox. The amount of time that the Security Escort System needs will drop dramatically, and it will continue to operate normally (same communications responses will be slowed by several hundred milliseconds).

No buddy check delay If checked, the software does not impose the hour between buddy checks from the same receiver. Normally, this checkbox is not checked and should not be checked for live systems.

No password to exit If checked, the software will exit without asking for a password. Normally, this checkbox is not checked.

No password on reentry If checked, the software will not ask for a password when the user switches to another program and then switches back to the still running Security Escort. Normally, this checkbox is not checked.

No password timeout If checked, the software will not ask for a password after the screen saver kicks in. Normally, this checkbox is not checked.

Bring to front on alarm If checked, the software will jump to the front when a new alarm occurs. Normally, this checkbox is checked.

Bring to front on trouble If checked, the software will jump to the front when a trouble dialog pops up. Normally, this checkbox is checked.

Control room output to siren If checked, whenever there is an unacknowledged alarm, the siren output on the control room output indicated below will operate.

Control room output to strobe If checked, whenever there is an unacknowledged alarm, the strobe output on the control room output indicated below will operate.

Control room output to spare If checked, whenever there is an unacknowledged alarm, the spare output on the control room output indicated below will operate.

Not always top window If the Security Escort System is intended to be the only application running on this computer, leave this checkbox unchecked. This will prevent other applications from taking over the screen. The Security Escort System will always be present. If the Security Escort System is to be run on a computer with other applications, check this checkbox and it will share the computer’s display like all other Windows applications. After checking this checkbox, stop and restart the Security Escort System for this feature to take effect. This checkbox is unchecked by default.

Excel test history files **Do not check this checkbox in a live Security Escort System.** It is for diagnostic Engineering testing only.

ID Receiver / Point

Assign a receiver for automated transmitter exchanges. The Security Escort System contains a feature where the transmitter identification number can be automatically entered into the **Subscriber Database**. This is used for entering transmitters when first issuing them to subscribers and for transmitter exchanges.

This automatic capture of the transmitter identification number is accomplished by performing certain procedural steps (see the Security Escort *Operation Manual*) and then using the transmitter to make a test transmission in close proximity to a designated receiver, usually located close to the Central Console. By capturing the transmitter identification number in this manner, keystroke errors are avoided during database entries and changes. The receiver chosen for this purpose is designated as the **ID Capture Receiver**. To assign the **ID Capture Receiver**, its transponder name and its **Point Number** are selected using the boxes labeled **ID Receiver** and **Point**.

Control room / Point

The Security Escort System Software can activate an output to attract attention when there is an alarm that has been received and no operator has responded to the system yet. To assign the control room output, select the transponder it is connected to, and its **Point Number**.

Map scale %

This value changes the scale that the maps are presented with. It is not intended for normal operation, but is typically used for testing to allow more of the map to be seen. The setting may range from 30% to 400%. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Alarm spot size

This setting changes the size of the yellow dot that marks the calculated location of the alarm. The settings range from 19 to 76 (half to double the default alarm dot size). It is best to set the size of the alarm spot so that represents a diameter of 15.24 m (50 ft.) on the displayed map, as this is the area where the transmission of the alarm most likely took place. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Linear depth

This setting controls the involvement of receivers in the alarm location calculation only when the “Linear Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. This setting should be changed if there are known problems with the location using the “Linear Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Low depth

This setting controls the involvement of receivers in the alarm location calculation only when the “Low Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Low Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Medium depth

This setting controls the involvement of receivers in the alarm location calculation only when the “Medium Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Medium Algorithm”. The **Enable Algorithm Tweaks** checcckbox must be checked for this to be displayed.

Strong depth

This setting controls the involvement of receivers in the alarm location calculation only when the “Strong Algorithm” is being used. The setting can range from 0 to 6 (default is 2). When set to 0, only the receivers closer to the actual location of the alarm will be considered in the location calculation. As the setting is raised, more distant receivers will be included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the “Strong Algorithm”. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Alarm zone

Four alarm zones allow the selection of which alarms from specific transmitters are reported on this workstation. This workstation displays the alarms only for the alarm zones that are checked. Each transmitter can be assigned to one or more alarm zones and when that transmitter generates an alarm (if this workstation has one or more of the same alarm zones checked), that alarm is displayed. The system defaults to all alarms displayed on all workstations.

[Save]

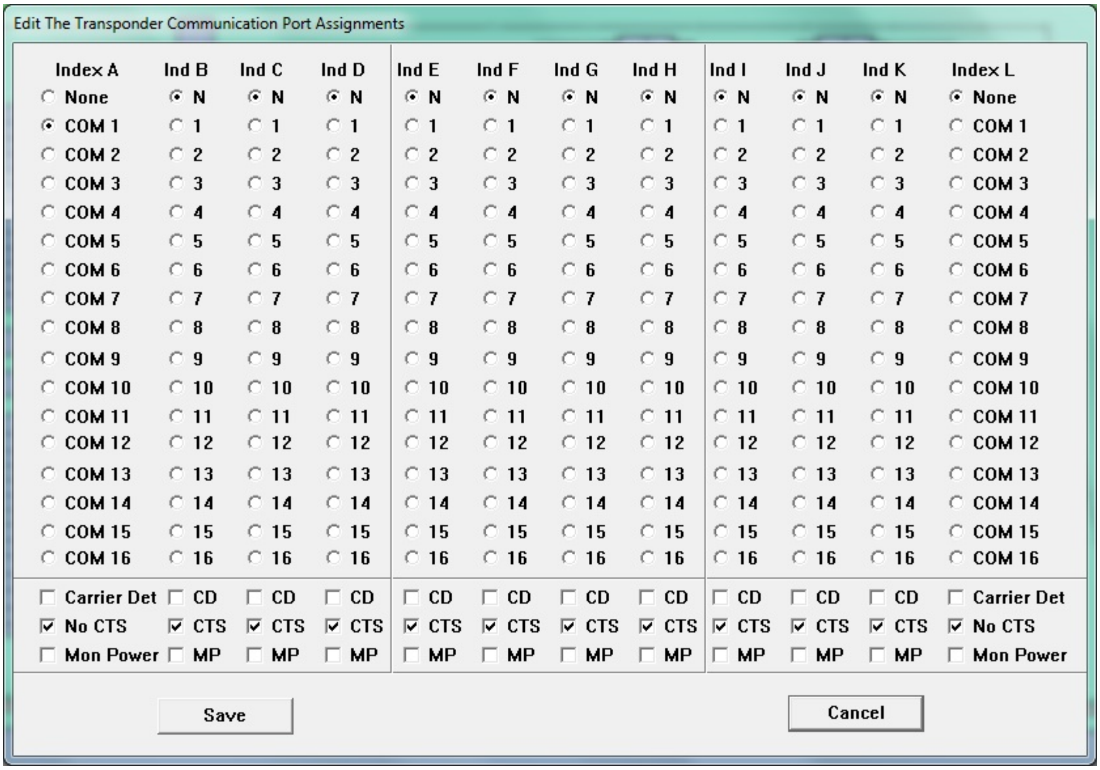
Save the changes and close the dialog window.

[Cancel]

Cancel the changes and close the dialog window.

4.3.13 Transponder comm port setup dialog

Go to menu **Setup > Transponder comm port setup...** This dialog connects the communication port indexes set for each transponder in the **Transponder Database** to the physical communication ports on the computer.



Edit The Transponder Communication Port Assignments

Index A	Ind B	Ind C	Ind D	Ind E	Ind F	Ind G	Ind H	Ind I	Ind J	Ind K	Index L
○ None	● N	● N	● N	● N	● N	● N	● N	● N	● N	● N	● None
● COM 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ 1	○ COM 1
○ COM 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ 2	○ COM 2
○ COM 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ 3	○ COM 3
○ COM 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ 4	○ COM 4
○ COM 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ 5	○ COM 5
○ COM 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ 6	○ COM 6
○ COM 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ 7	○ COM 7
○ COM 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ 8	○ COM 8
○ COM 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ 9	○ COM 9
○ COM 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ 10	○ COM 10
○ COM 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ 11	○ COM 11
○ COM 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ 12	○ COM 12
○ COM 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ 13	○ COM 13
○ COM 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ 14	○ COM 14
○ COM 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ 15	○ COM 15
○ COM 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ 16	○ COM 16
☐ Carrier Det	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ CD	☐ Carrier Det
☑ No CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ CTS	☑ No CTS
☐ Mon Power	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ MP	☐ Mon Power

Figure 4.44: Transponder Comm Port Setup dialog

COM The actual physical communication port over which communications to the transponder will be carried.

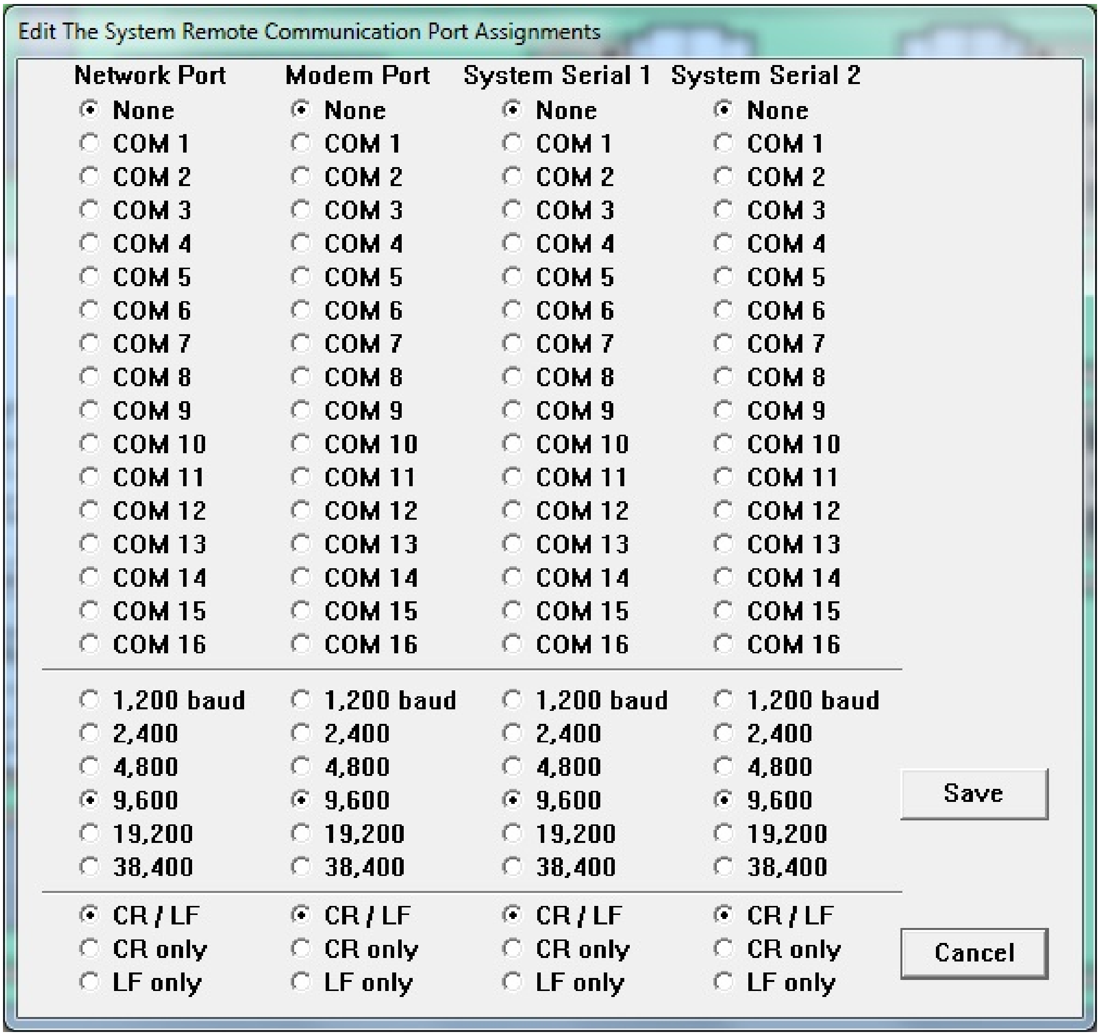
Carrier Det If checked, verify that the communications port is not in use before communicating. Only to be used on half duplex links where Carrier Detect indicates that the link is in use. This setting is normally unchecked and rarely used.

No CTS If checked, do not monitor the Clear to Send before communicating. This setting is normally checked.

Mon Power If checked, monitor the Ring Indicator pin to indicate a remote power supply used on this communication link has not failed. This setting is normally unchecked.

4.3.14 Remote comm port setup dialog

This dialog connects the network, modem and system serial ports to the physical communication ports on the computer and sets their baud rate.



Edit The System Remote Communication Port Assignments

Network Port	Modem Port	System Serial 1	System Serial 2
● None	● None	● None	● None
○ COM 1	○ COM 1	○ COM 1	○ COM 1
○ COM 2	○ COM 2	○ COM 2	○ COM 2
○ COM 3	○ COM 3	○ COM 3	○ COM 3
○ COM 4	○ COM 4	○ COM 4	○ COM 4
○ COM 5	○ COM 5	○ COM 5	○ COM 5
○ COM 6	○ COM 6	○ COM 6	○ COM 6
○ COM 7	○ COM 7	○ COM 7	○ COM 7
○ COM 8	○ COM 8	○ COM 8	○ COM 8
○ COM 9	○ COM 9	○ COM 9	○ COM 9
○ COM 10	○ COM 10	○ COM 10	○ COM 10
○ COM 11	○ COM 11	○ COM 11	○ COM 11
○ COM 12	○ COM 12	○ COM 12	○ COM 12
○ COM 13	○ COM 13	○ COM 13	○ COM 13
○ COM 14	○ COM 14	○ COM 14	○ COM 14
○ COM 15	○ COM 15	○ COM 15	○ COM 15
○ COM 16	○ COM 16	○ COM 16	○ COM 16
○ 1,200 baud	○ 1,200 baud	○ 1,200 baud	○ 1,200 baud
○ 2,400	○ 2,400	○ 2,400	○ 2,400
○ 4,800	○ 4,800	○ 4,800	○ 4,800
● 9,600	● 9,600	● 9,600	● 9,600
○ 19,200	○ 19,200	○ 19,200	○ 19,200
○ 38,400	○ 38,400	○ 38,400	○ 38,400
● CR / LF	● CR / LF	● CR / LF	● CR / LF
○ CR only	○ CR only	○ CR only	○ CR only
○ LF only	○ LF only	○ LF only	○ LF only

Figure 4.45: Remote Comm Port Setup Dialog

Network Port This port connects the master and slave computers of the Security Escort System. If this system has only a single computer, this setting should be set to none.

Modem Port This port typically connects to the modem for remote access and pager dial out. If set in the **Remote Setup** dialog, use this port without a modem for direct connection to a computer that is always on line.

System Serial 1/2 This is a general-purpose serial port. Its function is set up in the **Remote Setup** dialog.

COM The actual physical communication port over which these communications are carried.

Baud
The speed at which characters are transmitted on this serial port. This setting must match the baud rate of the device connected at the other end of this serial connection. This setting should always be at the highest speed that both connected devices have in common. Modem connections are typically much more efficient, if the baud rate is set significantly faster than the modems rated speed (for a 28.8 modem, set the baud rate to 57600 or 115200). The default setting is 9600 baud.

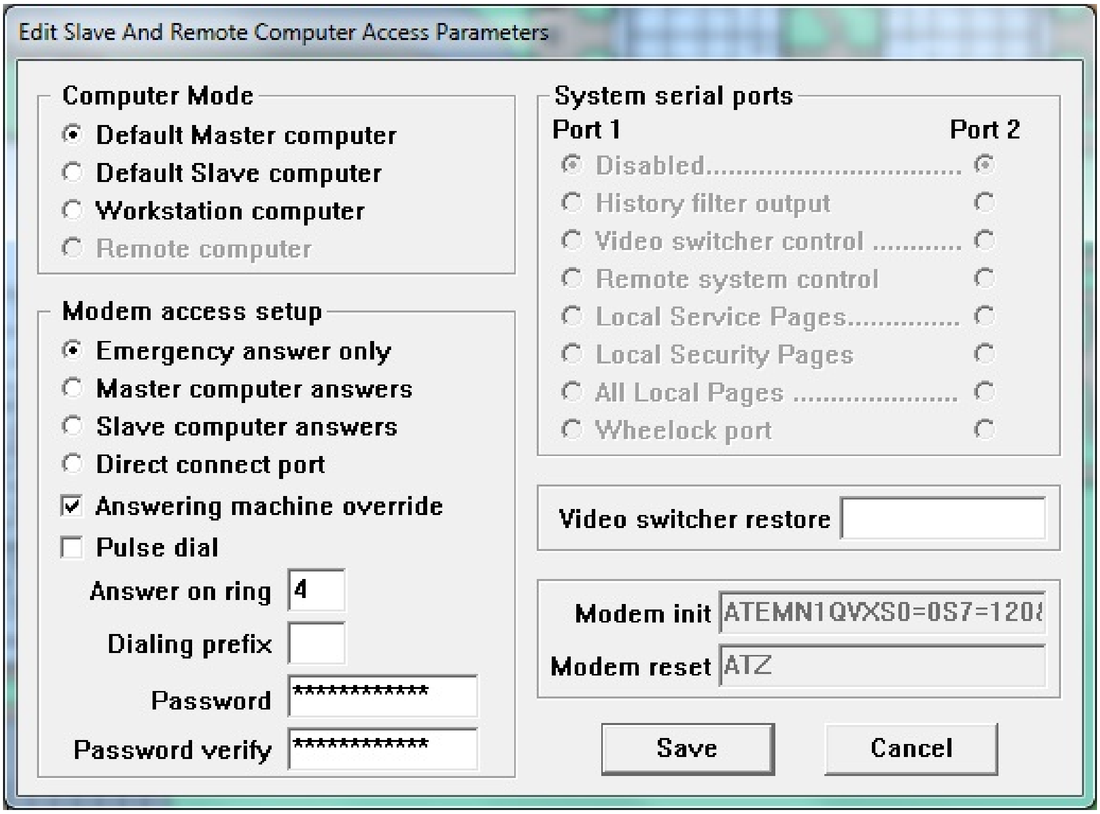
CR/LF
Appends carriage return and line feed characters at the end of each string transmitted (default). Only functions with the system serial ports (ignored on the network and modem ports).

CR Only
Appends a carriage return character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

LF Only
Appends a line feed character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

4.3.15 Remote setup dialog

This dialog sets up the remote access and system serial port parameters.



Edit Slave And Remote Computer Access Parameters

Computer Mode
- ● Default Master computer
- ○ Default Slave computer
- ○ Workstation computer
- ○ Remote computer

Modem access setup
- ● Emergency answer only
- ○ Master computer answers
- ○ Slave computer answers
- ○ Direct connect port
- ☑ Answering machine override
- □ Pulse dial

Answer on ring: 4
Dialing prefix:
Password: *************
Password verify: *************

System serial ports

Port 1		Port 2
●	Disabled................................	●
○	History filter output	○
○	Video switcher control	○
○	Remote system control	○
○	Local Service Pages...............	○
○	Local Security Pages	○
○	All Local Pages	○
○	Wheelock port	○

Video switcher restore:

Modem init: ATEMN1QVXS0=0S7=120
Modem reset: ATZ

Figure 4.46: Slave and Remote Computer Access Parameters Dialog

Default Master computer This computer is either the only computer in the system, or on startup, this computer defaults to the Master computer in a live Security Escort System.

Default Slave computer On startup, this computer defaults to the slave computer in a live Security Escort System.

Workstation computer This computer is used in a live Security Escort System for all operator functions. It cannot control the system like the Master and Slave computers.

Remote computer This computer is not in a live Security Escort System. It is used only for remote access. For this setting to be enabled, all transponder communication ports and the network port must be set to “None”.

Emergency answer only Allows the Master computer to answer a remote access only after 10 rings. If the Master does not answer, the Slave answers after 12 rings.

Master computer answers Allows the Master computer to answer a remote access after the programmed number of rings. If the Master does not answer, the Slave will answer after the programmed number of rings plus 2.

Slave computer answers Allows the Slave computer to answer a remote access after the programmed number of rings. If the Slave does not answer, the Master answers after the programmed number of rings plus 2. Generally, it is better to have the Master computer answer remote access calls.

Direct connect port The modem port is not connected to a modem. This setting will allow a direct connection to another computer. This additional computer will not display alarms, but otherwise will behave like a Slave computer.

Answering machine override If checked, an answering machine is connected to this phone line. If the answering machine answers a remote access call, hang up and redial. When another call is received within 1 min. of the last ring of a previous call, the Security Escort System will answer on the first ring, overriding the answering machine.

Pulse dial If checked, use pulse dial on all outgoing calls. Otherwise, tone dialing (default) is used.

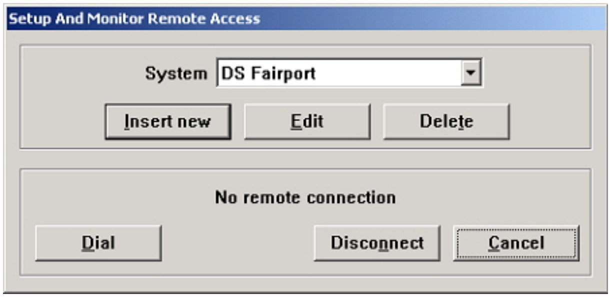
Answer on ring Program the number of rings on which to answer. If there is an answering machine on this phone line, set the number of rings to at least 2 greater than the number of rings the answering machine answers. Also check the **Answering Machine Override** checkbox.

Dialing prefix On outgoing calls, enter the dialing prefix, if any.

Password	This is the password that is used to gain remote access to the Security Escort System. If the first 5 characters of the password match the remote systems password, read only access will be allowed. If the first 8 characters match, you will be allowed to edit databases remotely (not currently implemented). If all 12 characters match, you will also be allowed to change system parameters remotely.
Password verify	For verification, reenter the same password as above.
Disabled	If selected, this system serial port is disabled (default).
History filter output	If selected, this system serial port sends out whatever items that are selected in the **History Filter** dialog.
Video switcher control	If selected, this system serial port sends out the strings programmed in the **Video Switcher** field of the **Transponder Database Edit** dialog's **Area** data. Also see **Video switcher restore** field below.
Remote system control	If selected, this system is controlled by another system through a proprietary protocol. This setting can only be used when two systems are specifically designed to work together.
Local Service Pages	If selected, system will send service pages via the local port.
Local Security Pages	If selected, system will send security pages via the local port.
All Local Pages	If selected, system will send both service and security pages via the local port.
Video switcher restore	This string is transmitted on any system serial port programmed for **Video switcher control** when all alarms are restored. This string is transmitted to the video switcher to reset it to the default displays. Up to 20 characters can be entered. Control characters can be entered as [^][A] for control A.
Modem init	This is the initialization string transmitted to the modem to set it up for all communications except paging. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift> + <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.
Modem reset	This is the reset string transmitted to the modem. Normally, this setting does not need to change. To allow changes to this string, hold down the <Shift>+ <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default string should work with most modems.
[Save]	Save the changes and close the dialog window.
[Cancel]	Cancel the changes and close the dialog window..

4.3.16 Remote connection dialog

This dialog sets up the remote access parameters that allow remote connection to a live Security Escort System.



System DS Fairport

No remote connection

Figure 4.47: Remote Connection Dialog

Set the modem port and speed in the **Remote comm port setup** dialog. The speed selected should be greater than the speed of the modem and the same as the speed selected for the remote system. Use the **Backup** command under the **Utilities menu** to create a database backup to a disk. In the **Remote setup** dialog, assign a password and set which computer (Master or Slave) is to answer and the number of rings to answer on. Also copy the map files from the live Security Escort System. The map is in the “Escort” sub-directory and is named MAP0.EDB. There may also be other maps with the names MAP1.EDB, MAP2.EDB, and so on.

In the Security Escort System used for remote access

This dialog sets up the remote access parameters that allow remote connection to a live Security Escort System.

1. Program all communication port indexes in the **Transponder comm port setup** dialog to “None”.
2. In the **Remote comm port setup** dialog, set the network port to “None” and set the modem to the communication port of the modem. The speed selected should be greater than the speed of the modem, and the same as the speed of the live system that is being called.
3. In the **Remote setup** dialog, set the Master/Slave/remote setting to remote.
4. In the **Remote connection** dialog, select the **[Insert new]** button and enter a name, password, phone number, and three-character file extension for this system’s database files. Using a disk written with the **Backup** command of the system you desire access to, restore the database files. Select the system you just entered from the drop-down list in the **Remote connection** dialog. Exit the **Remote connection** dialog.
5. Select **Restore** menu item under the **Utilities** menu. Restore from the backup disk to each database. When completed, you should also store a copy of the map file in the “Escort” sub-directory under the name MAP0.xxx, (where xxx is the three-character file extension entered earlier).
6. In the **Remote connection** dialog, click the **[Dial]** button to call the remote system. If the first 5, 8, or 12 characters of the password match, you can enter the system.

[Insert new]	Clicking this button presents a blank **Phone Book Edit** dialog to enter a new remote access Security Escort System.
[Edit]	Selecting the desired Security Escort System and then clicking this button allows the existing Security Escort System data to be edited.
[Delete]	Selecting the desired Security Escort System and then clicking this button deletes the data for the selected Security Escort System.

[Dial]
Selecting the desired Security Escort System and then clicking this button attempts to connect the selected Security Escort System. This selection is only available on the remote computer; it is not available on a live Security Escort system.

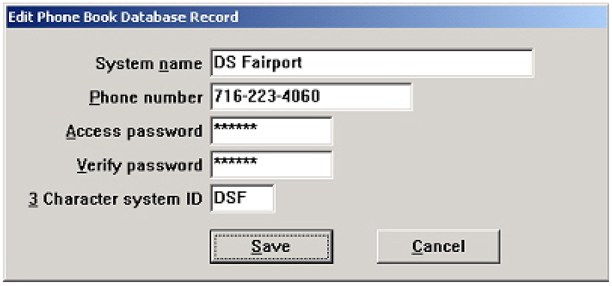
[Answer]
This option is only available in a live Security Escort System. Clicking this button manually answers an incoming call from a remote Security Escort System.

[Disconnect]
Clicking this button drops a remote connection. This can be done either on the live system or the remote access system.

[Cancel]
Clicking this button closes this dialog, but does not disconnect a remote access connection. At this point, you can navigate the menus and screens on the remote system as if you were at the on-site slave computer system. To drop the connection, return to this dialog and click the **[Disconnect]** button.

Phone Book Edit dialog

This dialog edits existing entries and adds new phone book entries for remote system access.



Edit Phone Book Database Record

System name: DS Fairport
Phone number: 716-223-4060
Access password: ******
Verify password: ******
3 Character system ID: DSF

Figure 4.48: Phone Book Edit Dialog

System name
This is a reference name for the Security Escort System to be accessed remotely. This is the name of the desired system to be accessed in the **Remote connection** dialog.

Phone number
The phone number to be dialed to access the Security Escort System. Enter a comma for each 2 sec. pause desired.

Access password
This is the password used to gain access to the remote Security Escort System. On the live system being dialed into, set the remote password in the **Remote Setup** dialog. If the first 5 characters of the password match, the remote system allows read only access. If all 12 characters match, you can change system parameters remotely.

Verify password
For verification, retype the password entered into the **Access Password** textbox.

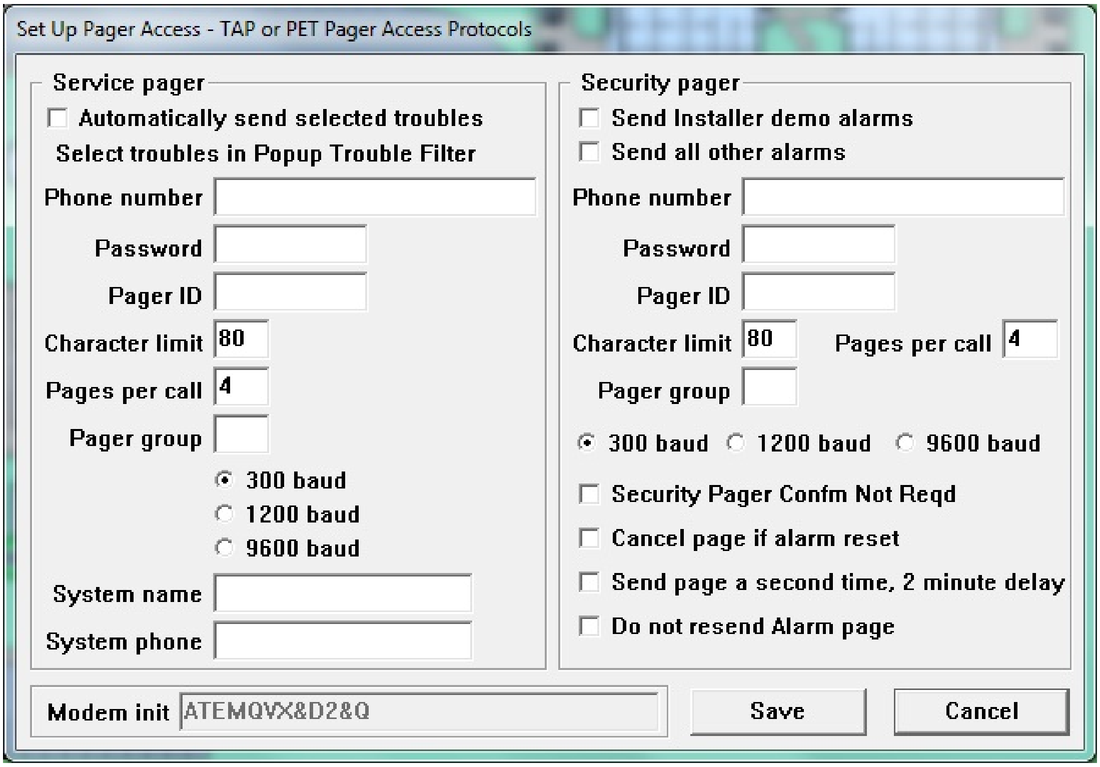
3 Character system ID
Enter a unique three character ID that is used as an extension to the map and database files for accessing this Security Escort System.

[Save] Save the changes and close the dialog window.

[Cancel] Cancel the changes and close the dialog window.

4.3.17 Pager setup dialog

This dialog sets up remote pager access for troubles (service) and alarms (security).



Set Up Pager Access - TAP or PET Pager Access Protocols

Service pager

☐ Automatically send selected troubles

Select troubles in Popup Trouble Filter

Phone number

Password

Pager ID

Character limit 80

Pages per call 4

Pager group

● 300 baud

○ 1200 baud

○ 9600 baud

System name

System phone

Security pager

☐ Send Installer demo alarms

☐ Send all other alarms

Phone number

Password

Pager ID

Character limit 80 Pages per call 4

Pager group

● 300 baud ○ 1200 baud ○ 9600 baud

☐ Security Pager Confm Not Reqd

☐ Cancel page if alarm reset

☐ Send page a second time, 2 minute delay

☐ Do not resend Alarm page

Modem init ATEMQVX&D2&Q

Figure 4.49: Pager Setup Dialog

Automatically send selected troubles If checked, send the troubles selected in the **Popup trouble filter** dialog to the service pager.

Phone number Phone number to be dialed to access the paging service. This phone number is usually different from the number you would manually dial to send a page. The paging company assigns this value.

Password This is the password that must be sent to the paging service to send the page. If not required, leave this field black. Usually a password is not required. The paging company assigns this value.

Pager ID This is the ID that identifies the specific pager that this message is to be sent to. Many times, it is the last 7 digits of the phone number that you would manually dial to access this pager. The paging company assigns this value.

Character limit This is the maximum number of characters allowed per page. Typically, this is set to 80 characters. The Security Escort System will truncate the pager message at this number of characters. The paging company assigns this value.

Pages per call
This is the maximum number of pager messages allowed per phone call. Typically, this is set to 4 pages per call. When this number of messages have been sent, and there are more messages to be delivered; the Security Escort System will hang up and redial the paging service to deliver the remaining messages. The paging company assigns this value.

Pager group
This is the group of up to 8 pagers that this message is to be sent to. You may program the individual pager as well as a group of pagers. The pager group will be sent the page before the individual.

Baud rate
This is the baud rate that will be used to communicate with the paging computers. The paging company assigns this value.

System name
This identifies the Security Escort System when multiple Security Escort Systems report to the same service pager. Keep this field as short as reasonably possible since these characters, including space character, will be sent before each trouble message and they are included in the **Character limit** set above. If not desired, leave blank.

System phone
This will present phone number to be called in response to the service page. Only use if required since these characters, plus a space, will be sent before each trouble message. They are included with the **System name** in the **Character limit** set above. If not desired, leave blank.

Send installer demo alarms
If checked, demo alarms will be sent to the security pager.

Send all other alarms
If checked, all actual alarms will be sent to the security pager.

Security Pager Confm Not Reqd
If checked, the confirmation pager message is not sent to the security pager when the alarm is acknowledged by an acknowledgement transmitter.

Cancel page If alarm reset
If checked, the alarm page will be canceled if the alarm is reset before it can be communicated to the paging service.

Send page a second time, 2 minute delay
If checked an alarm page will be sent a second time to the security pager. Do this in case the pager was in an area where pages could not be heard when the first page was sent.

Do not resend alarm page
If checked, a pager message is sent to the security person only once till the alarm is cancelled or acknowledged.

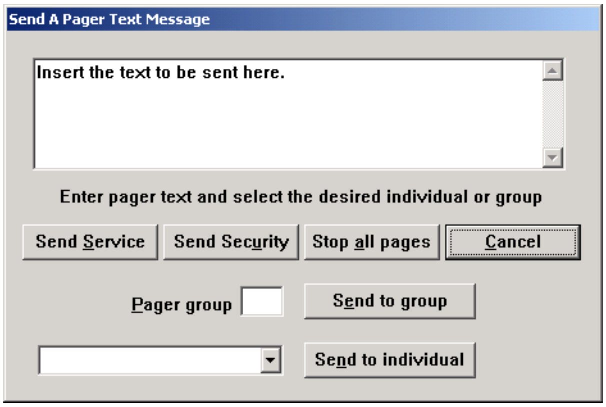
Modem init
This is the initialization string sent to the modem to set it up for pager communications. Normally, this setting would not have to be changed. To allow changes to this string, hold down the <Shift> + <Ctrl> keys when this dialog is first opened. This string is specific to each modem model. The default setting should work with most modems.

[Save]
Save the changes and close the dialog window.

[Cancel]
Cancel the changes and close the dialog window.

4.3.18 Send pager message dialog

Allows manually entered messages to be sent to the service or security pagers. Service and security pagers are configured in the **Pager setup** dialog. Individuals and group pager assignments are configured in the **Subscriber Database**.



Send A Pager Text Message

Insert the text to be sent here.

Enter pager text and select the desired individual or group

Figure 4.50: Send Pager Message Dialog

Insert the text to be sent here. Enter the text to be sent to the pagers in the large text box at the top of the dialog.

[Send Service] Causes the entered message to be sent to the service pager and service pager group.

[Send Security] Causes the entered message to be sent to the security pager and security pager group.

[Stop all pages] Causes all pages currently queued (automatic or manual) to be aborted and deleted. Use with caution.

Pager group To send a page to all members of a group, enter the pager group number here (1 to 99).

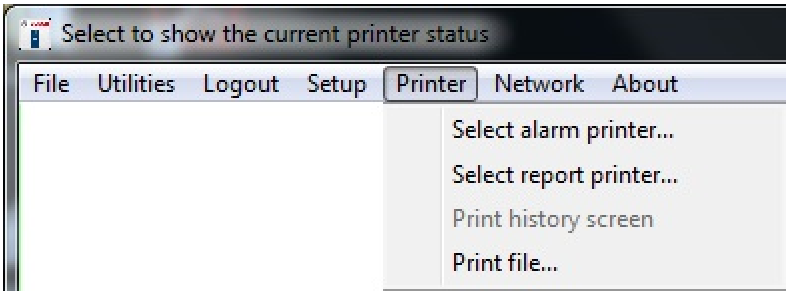
[Send to group] Click this button to send the text entered to the indicated pager group.

[Send to Individual] Click this button to send the text entered to the individual that is selected from the drop down list.

[Cancel] Cancel and close this dialog window..

4.4 Printer menu

The printer menu allows the alarm and report printers to be setup and enabled. You can also print the contents of the history screen and files.

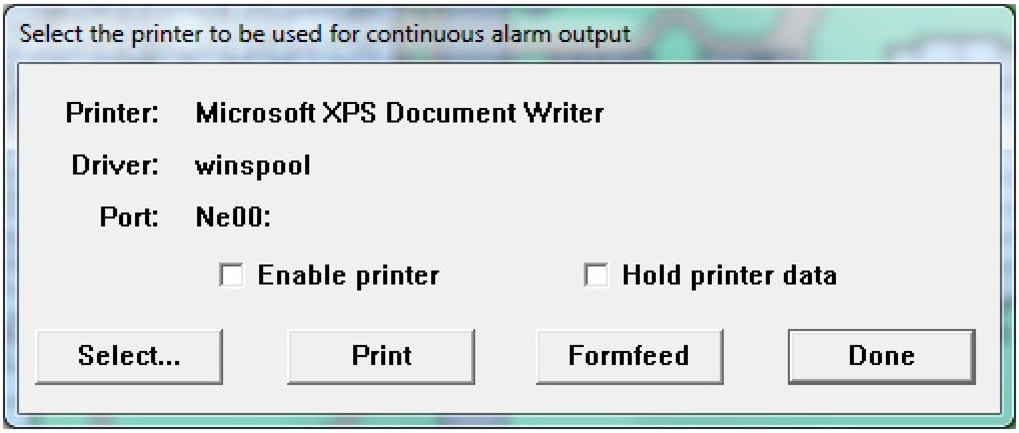


Select to show the current printer status

Figure 4.51: Printer menu

4.4.1 Select alarm printer dialog

The alarm printer is used to print all real time event data (alarm, tests, troubles and so on) as they happen. Typically, the alarm printer is a continuous form printer and not a page at a time printer such as a laser printer.



Select the printer to be used for continuous alarm output

Printer: Microsoft XPS Document Writer

Driver: winspool

Port: Ne00:

□ Enable printer □ Hold printer data

Figure 4.52: Alarm Printer Dialog

Enable printer Check this checkbox to allow the system to send the real time events to the selected alarm printer.

Hold printer data Check this checkbox to force the system to hold the data and not send it to the selected alarm printer. This is not recommended operation, but it allows a page at a time printer to be used as an alarm printer. Use the **[Print]** button to force the data to print on demand.

[Select] Click this button to present the Window’s system printer selection window. This window is used to select the alarm printer from all of the printers that are installed on this computer.

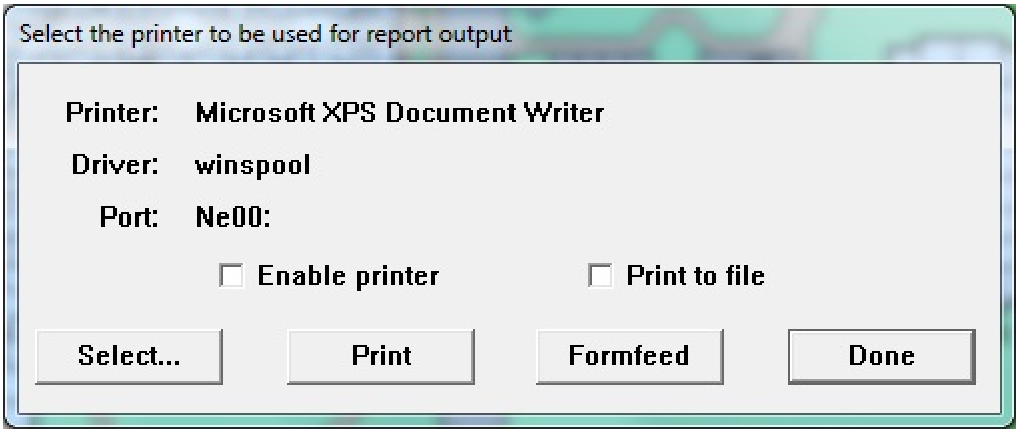
[Print] Click this button to print the data that is currently held in Security Escort’s alarm printer buffer.

[Formfeed] Click this button to send a formfeed to the alarm printer.

[Done] Click this button to close the dialog window.

4.4.2 Select report printer dialog

The report printer is used to print all reports as they are requested automatically or by the operator. Typically, the report printer is a page at a time printer like a laser printer.



Select the printer to be used for report output

Printer: Microsoft XPS Document Writer

Driver: winspool

Port: Ne00:

□ Enable printer □ Print to file

Figure 4.53: Report Printer Dialog

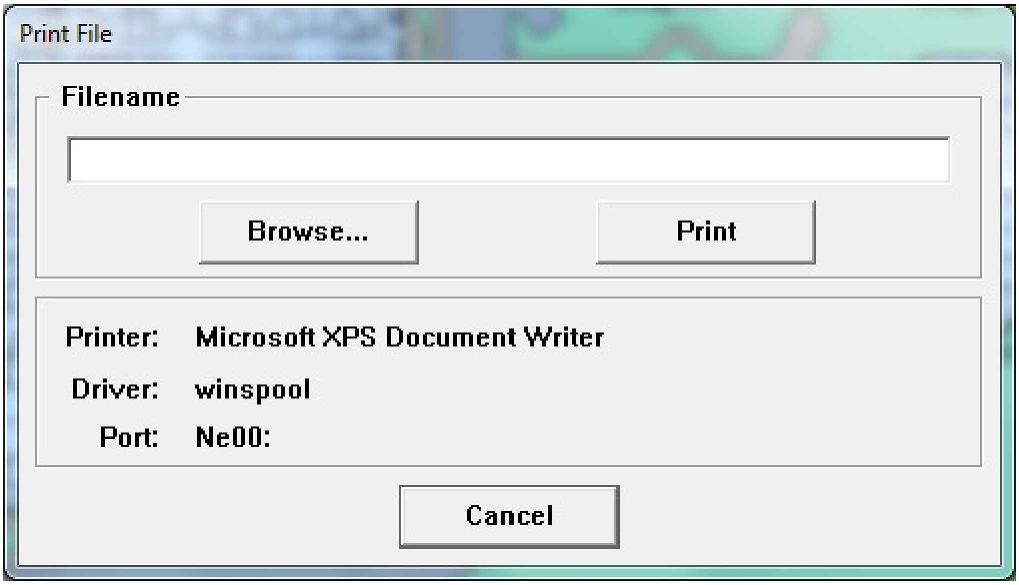
Enable printer	Check this checkbox to allow the system to send the reports to the selected report printer.
Print to file	Check this checkbox to create file copies of all reports. This option is independent of the report printer, which can also be used at the same time.
[Select...]	Click this button to present the Window's system printer selection window. This window is used to select the report printer from all of the printers that are installed on this computer.
[Print]	Click this button to print the data that is currently held in Security Escort's report printer buffer.
[Formfeed]	Click this button to send a formfeed to the report printer.
[Done]	Click this button to close the dialog window.

4.4.3 Print history screen

This selection will print the current data in the **History Screen** buffer to the report printer.

4.4.4 Print file dialog

Enter the name of the file to be printed or click the **[Browse...]** button to open the **Common Open File** dialog. Then click the **[Print]** button to print the file to the report printer.



Printer: Microsoft XPS Document Writer
Driver: winspool
Port: Ne00:

Figure 4.54: Print File Dialog

This is the standard Windows **Common Open File** dialog that is used for selecting the file to be printed. It works the same as any other Window's standard application.

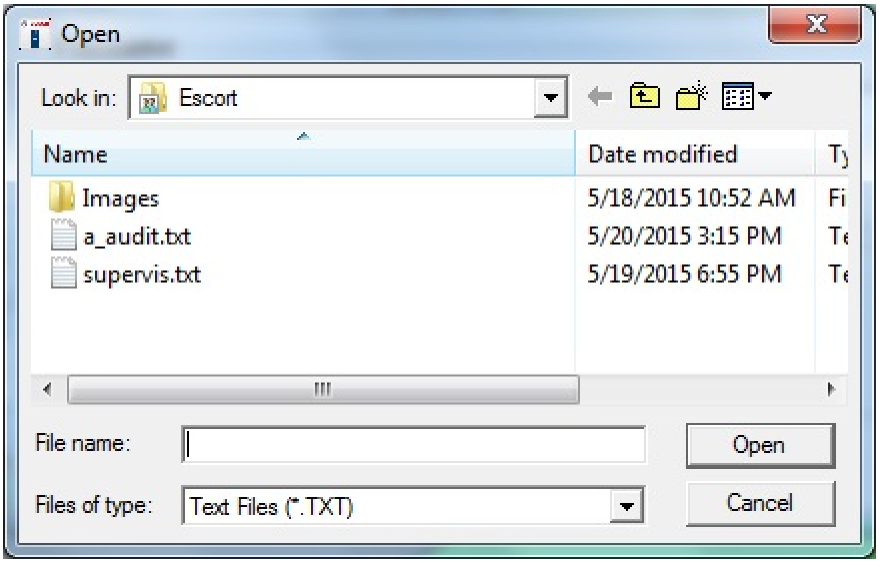


Figure 4.55: Common Open File Dialog

4.5 Network menu

This is the network menu used to set up and monitor the TCP/IP network and the computer’s file paths.

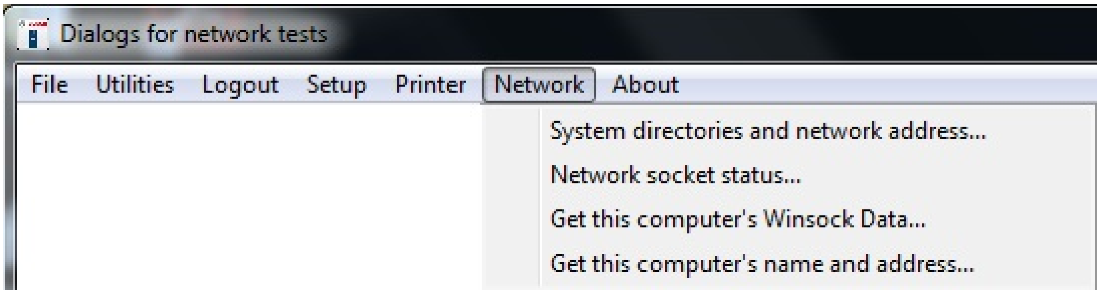
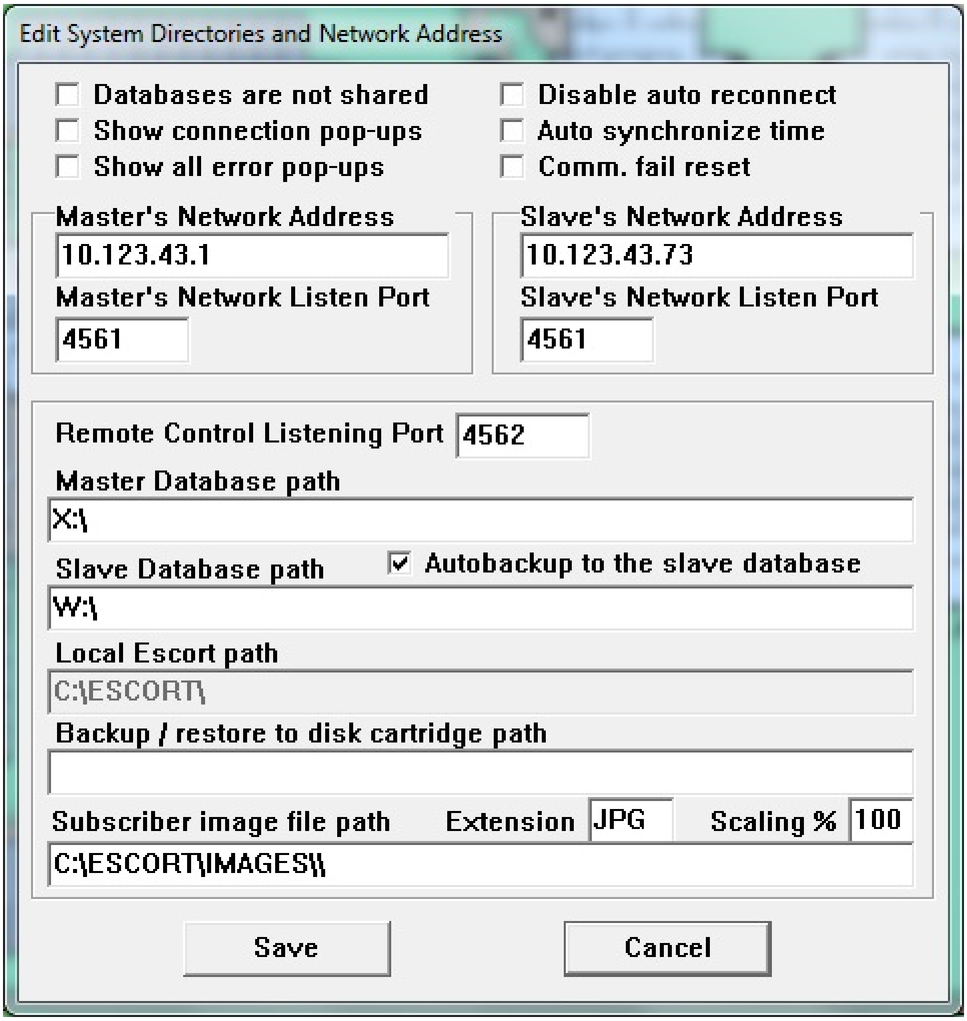

Dialogs for network tests
File
Utilities
Logout
Setup
Printer
Network
About
System directories and network address...
Network socket status...
Get this computer's Winsock Data...
Get this computer's name and address...

Figure 4.56: Network Menu

4.5.1 System directories and network address dialog

Use this dialog to set up the network IP addresses, ports and related options. File paths can also be configured.



Edit System Directories and Network Address

□ Databases are not shared
□ Show connection pop-ups
□ Show all error pop-ups
□ Disable auto reconnect
□ Auto synchronize time
□ Comm. fail reset

Master's Network Address: 10.123.43.1
Master's Network Listen Port: 4561
Slave's Network Address: 10.123.43.73
Slave's Network Listen Port: 4561

Remote Control Listening Port: 4562
Master Database path: X:\
Slave Database path: W:\
☑ Autobackup to the slave database
Local Escort path: C:\ESCORT\
Backup / restore to disk cartridge path:
Subscriber image file path: C:\ESCORT\IMAGES\\
Extension: JPG
Scaling %: 100

Figure 4.57: System Directories and Network Address Dialog

Databases are not shared If this option is not checked, the master and all the slave and workstation computers share the same database files. This checkbox must only be checked if each computer has its own copy of the databases stored locally. In normal operation, this checkbox is typically unchecked. If this checkbox is checked, the databases must be manually updated using **Backup** and **Restore** every time changes are made to the database.

Show connection pop-ups If this option is checked, it will display a pop-up message box whenever a network connection is initiated or released with another computer. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked.

Show all error pop-ups If this option is checked, it will display a pop-up message box whenever a network error is reported. Unchecking this checkbox stops the message boxes from displaying. In normal operation, this checkbox is typically unchecked.

Disable auto reconnect If this option is checked, the system will not automatically attempt to reconnect a lost connection each minute. Unchecking this checkbox allows the system to automatically reconnect a lost connection. In normal operation, this checkbox should be unchecked.

Auto synchronize time If this option is checked, the master computer will automatically synchronize the time on the slave and workstation computers once each night.

Comm. fail reset If this option is checked, the master computer will reset when communication failure occurs..

Master’s Network Address: The IP address of the master computer. The Security Escort system requires a fixed IP address for the master computer.

Master's Network Listen Port A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set as “4561”.

Slave's Network Address The IP address of the slave computer. The Security Escort system requires a fixed IP address for the optional slave computer.

Slave's Network Listen Port A unique number that indicates the Security Escort software is attempting to set up a connection. Other software uses different port numbers, allowing the network interface card to be shared with other network applications. Typically, this is set to “4561”.

[Learn address] Clicking this button on the master computer automatically populates the master’s IP address in the **Master’s Network Address** textbox, and the master’s network port in the **Master’s Network Listen Port** textbox. Clicking this button on the slave computer automatically populates the master’s IP address in the **Slave’s Network Address** textbox, and the master’s network port in the **Slave’s Network Listen Port** textbox. If the computer has more than one network interface card (NIC), you must verify that the correct IP address was selected by comparing this address to the IP address that was programmed in the Control Panel TCP/IP protocol. If the address is not correct, manually enter the correct IP address.

Remote Control Listening Port
The Security Escort will be listening on this port to communicate with the OPC server. A separate OPC server is created to communicate between the OPC client and the Security Escort system. The OPC server holds the alarm and trouble messages, and sends the same to the available client once it is connected. The OPC server will send the status of the Security Escort to the OPC client. The OPC sever also acknowledges and deletes alarm and trouble messages from OPC client. If the connection between OPC server and Security Escort goes down, the OPC server will try to reconnect with Security Escort. Once the connection to the Security Escort becomes active, the Security Escort will send all the available alarms to the OPC server. The OPC server in turn sends the alarm back to OPC client; hence the OPC client may display some duplicate alarms.

Master Database path
The path that this slave or workstation computer uses to access the shared database files on the master computer. This path may have a different drive letter on the different slave and workstation computers. They are typically on the master computer, but they may be on a file server or any other network accessible drive. **Note: With version 2.04 and above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the master computer's database would be "\\MASTER\ESCORT".**

Autobackup to the slave database
If this option is checked, the slave computer will back up all databases in the **Master Database path** to the **Slave Database path** each night at 3:00 am.

Slave Database path
The path that this master or workstation computer uses to access the hot backup database files on the slave computer. This path may have a different drive letter on the different master and workstation computers. They are usually on the slave computer, but they may be on a file server or any other network accessible drive. Typically, they would not be stored on the same computer as the **Master Database path**, so a single failure would not prevent access to both the master and slave database files.
Note: With version 2.04 or above of the software, it is possible to use UNC path names instead of mapping drive letters. Therefore, the path to the slave computer's database would be "\\SLAVE\ESCORT".

Local Escort path
The path on this workstation where the Security Escort was installed in. Typically it is "C:\ESCORT".

Backup / restore to disk cartridge path
When backing up or restoring the databases to a disk cartridge, this is the path that is used.

Subscriber image file path
The Security Escort System software can display an image for each subscriber on the alarm screen. This parameter tells the software the path where the image files are stored. The default is "C:\ESCORT\IMAGES".

Extension The subscriber images can be in JPEG or Windows Bitmap format. All images in a system must be in the same format. For the JPEG format, enter the Windows extension “JPG”. For the Bitmap format, enter the Windows extension “BMP”.

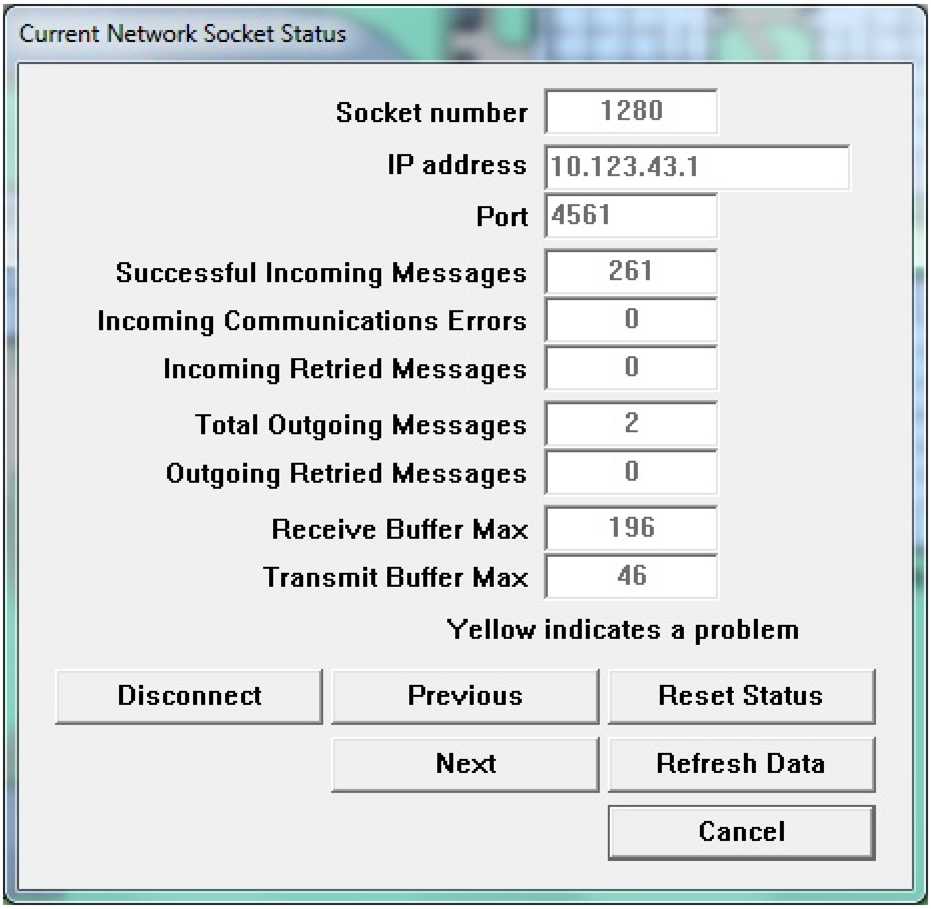
Scaling % When the display is set to 640x480 pixels, and subscriber images are being displayed, this parameter controls the image size. This value can range from 10 to 100%, and should be adjusted while viewing alarms to get the desired image size. When the display is set to 800x600 or larger (recommended), this parameter has no effect.

[Save] Clicking this button saves the changes and closes the dialog window.

[Cancel] Clicking this button aborts the changes and closes the dialog window.

4.5.2 Network socket status dialog

This dialog shows diagnostic information for the selected TCP/IP socket.



Current Network Socket Status

Socket number: 1280
IP address: 10.123.43.1
Port: 4561
Successful Incoming Messages: 261
Incoming Communications Errors: 0
Incoming Retried Messages: 0
Total Outgoing Messages: 2
Outgoing Retried Messages: 0
Receive Buffer Max: 196
Transmit Buffer Max: 46

Yellow indicates a problem

Figure 4.58: Current Network Socket Status Dialog

Successful Incoming Messages Number of messages that the system has successfully received on this socket.

Incoming Communication Errors Number of messages that the system detected errors in, on this socket. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.

Incoming Retried Messages Number of successful receptions which indicated that the retries by the sending application. If displayed in yellow, this value is more than 1.5% of the **Successful Incoming Messages**.

Total Outgoing Messages Total number of outgoing messages that were sent on this socket.

Outgoing Retried Messages Number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the **Total Outgoing Messages**.

Receive Buffer Max Maximum number of bytes that were received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

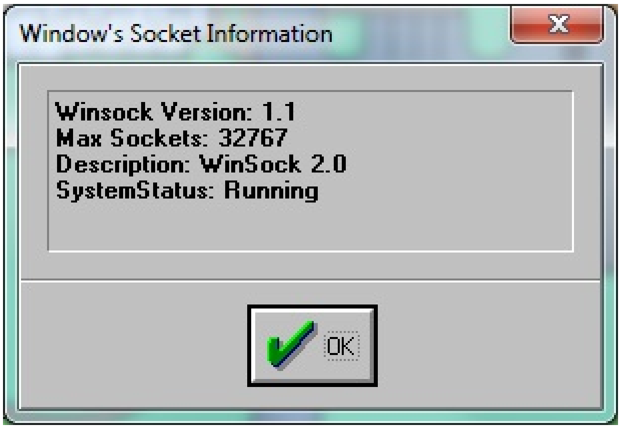
Transmit Buffer Max Maximum number of bytes that were processed by the system, but not yet transmitted on this socket. If displayed in yellow, more than 50% of the queue was in use.

[Reset Status] Clicking this button resets all values shown in this dialog.

[Refresh Data] Clicking this button refreshes all values shown in this dialog. The values are not automatically updated when the dialog is left open.

4.5.3 Computer’s Winsock data dialog

This dialog shows information about the Windows Winsock support. This is only used for diagnostic purposes.

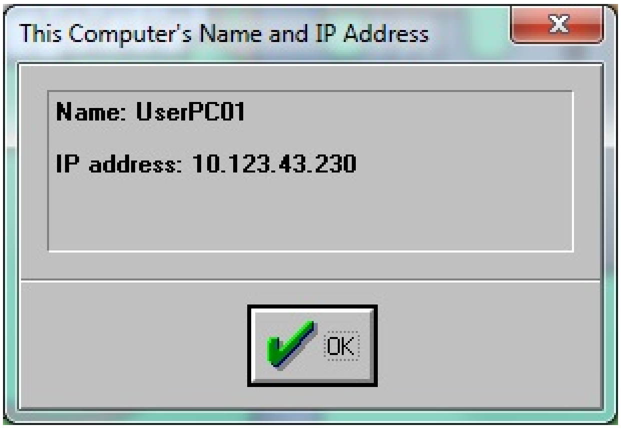


Winsock Version: 1.1
Max Sockets: 32767
Description: WinSock 2.0
SystemStatus: Running

Figure 4.59: Computer’s Winsock Data Dialog

4.5.4 Computer's name and address dialog

This dialog shows the computer’s network name and current IP address.



Name: UserPC01

IP address: 10.123.43.230

Figure 4.60: Computer's Name and IP Address Dialog

4.6 About menu

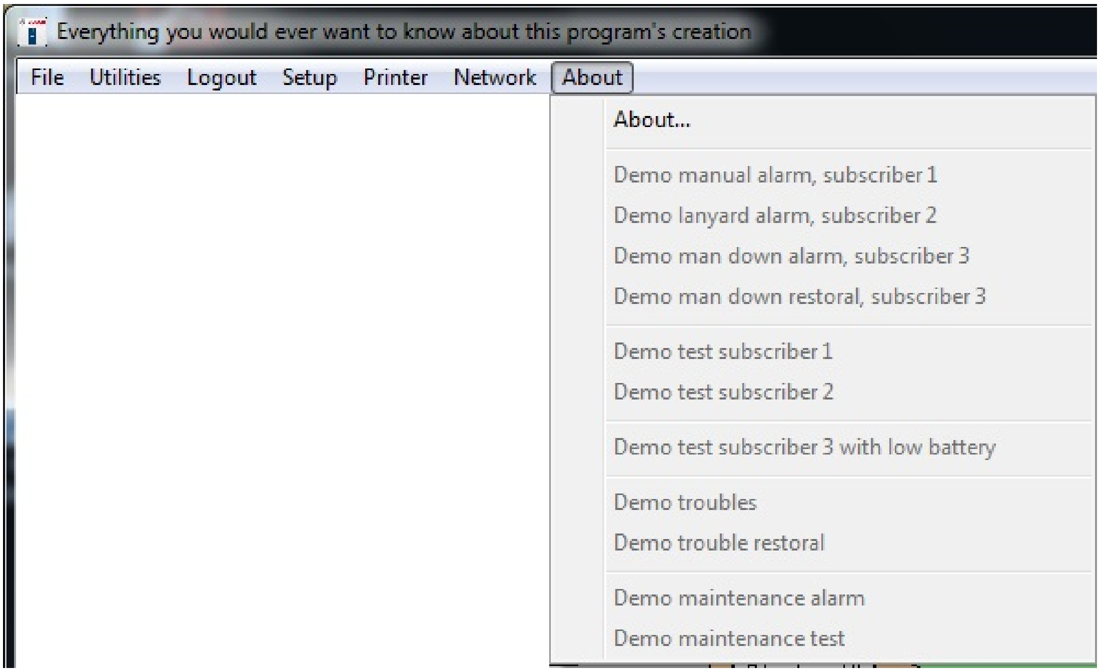

Everything you would ever want to know about this program's creation
File
Utilities
Logout
Setup
Printer
Network
About
About...
Demo manual alarm, subscriber 1
Demo lanyard alarm, subscriber 2
Demo man down alarm, subscriber 3
Demo man down restoral, subscriber 3
Demo test subscriber 1
Demo test subscriber 2
Demo test subscriber 3 with low battery
Demo troubles
Demo trouble restoral
Demo maintenance alarm
Demo maintenance test

Figure 4.61: About Menu

Demo manual alarm, subscriber 1
For demonstration only, and can’t be used in a live system. It causes system to display an alarm from the subscriber with transmitter ID number 1. In the **System Preferences** dialog, select **Enable Demo Selections** checkbox to enable these demo alarm and trouble selections. The transponder communication ports and network communication ports must also be disabled, and the operator of the system must login at “Installer” or “Installer Master” authority level.

Demo lanyard alarm, subscriber 2
For demonstration only, and can’t be used in a live system. It causes system to display a lanyard alarm from the subscriber with transmitter ID number 2.

Demo man down alarm, subscriber 3
For demonstration only, and can’t be used in a live system. It causes system to display a man down alarm from the subscriber with transmitter ID number 3. The man down alarm is delayed by the programmed man down delay (usually 10 seconds).

Demo man down restoral, subscriber 3
For demonstration only, and can’t be used in a live system. It will restore a previous man down alarm from the subscriber with transmitter ID number 2, if it has not timed out and is not being displayed.

Demo test subscriber 1
For demonstration only, and can’t be used in a live system. It simulates a test from the subscriber with transmitter ID number 1.

Demo test subscriber 2
For demonstration only, and can’t be used in a live system. It simulates a test from the subscriber with transmitter ID number 2.

Demo test subscriber 3 with low battery
For demonstration only, and can’t be used in a live system. It simulates a test from the subscriber with transmitter ID number 3. This test also reports low battery.

Demo troubles
For demonstration only, and can’t be used in a live system. It simulates troubles from a transponder. Point troubles are simulated for AC loss, tamper and no response. Transponder troubles are simulated for remote key and remote key tamper. The individual troubles can be enabled or disabled in the **Popup Trouble Filter** dialog. The trouble delay in the **Popup Trouble Filter** dialog will also affect these troubles. Therefore, for demo purposes, it should be set to 0.

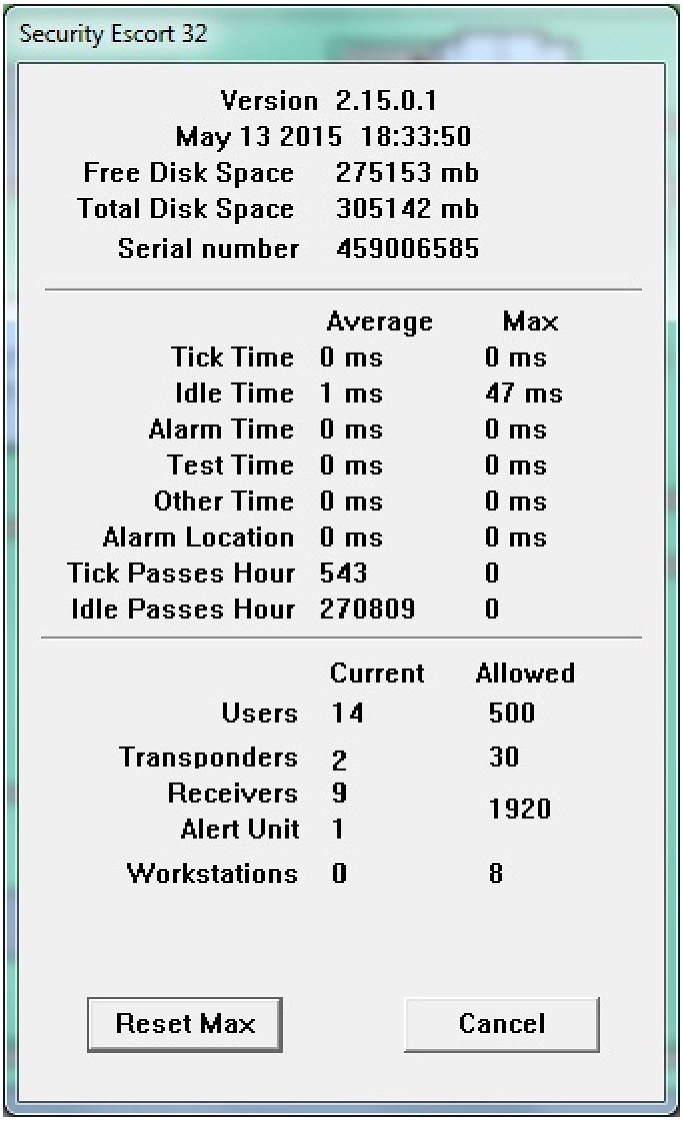
Demo trouble restoral
For demonstration only, and can’t be used in a live system. It simulates trouble restorals for all the troubles sent in **Demo Troubles**.

Demo maintenance alarm
For demonstration only, and can’t be used in a live system. It simulates an alarm from a maintenance transmitter.

Demo maintenance test
For demonstration only, and can’t be used in a live system. It simulates a test from a maintenance transmitter.

4.6.1 About dialog

The **About** dialog presents the version information, copyright data and internal processing timers.



Version 2.15.0.1
May 13 2015 18:33:50

Free Disk Space	275153 mb
Total Disk Space	305142 mb
Serial number	459006585

	Average	Max
Tick Time	0 ms	0 ms
Idle Time	1 ms	47 ms
Alarm Time	0 ms	0 ms
Test Time	0 ms	0 ms
Other Time	0 ms	0 ms
Alarm Location	0 ms	0 ms
Tick Passes Hour	543	0
Idle Passes Hour	270809	0

	Current	Allowed
Users	14	500
Transponders	2	30
Receivers	9	1920
Alert Unit	1	
Workstations	0	8

Figure 4.62: About Dialog

Version
At the top of the dialog, the software version and the date and time that it was compiled, is displayed.

Free Disk Space
This shows the free disk space on the “C” drive of this computer.

Total Disk Space
This shows the total disk space on the “C” drive of this computer.

Tick Time
The amount of time spent in the time tick processor per pass.

Idle Time
The amount of time spent In the idle time processor per pass.

Alarm Time
The amount of time spent to process each alarm report from a transponder.

Test Time
The amount of time spent to process each test report from a transponder.

Other Time
The amount of time spent to process each trouble and other message reports from a transponder.

Alarm Location
The amount of time spent to compute an alarm location.

Tick Passes Hour
The number of passes through the tick time processor that occurred in an hour.

Idle Passes Hour
The number of passes through the idle time processor that occurred in an hour.

Serial number
Displays the serial number of this Security Escort System installation as read from the software key.

Maximum users
Displays the maximum number of users that this Security Escort System installation allows. This number is programmed into the software key.

Max transponders
Displays the maximum number of transponders that this Security Escort System installation allows. This number is programmed into the software key.

Max workstations
Displays the maximum number of workstations that this Security Escort System installation allows. This number is programmed into the software key.

[Reset Max]
Resets all of the max timers.

5 Image files

Map file generation and scaling

The Security Escort maps are standard Windows bitmap files (.BMP). MAP0.EDB is the default map file, usually the ground floor in multiple map systems. The map must be saved in the Security Escort subdirectory (typically “C:\ESCORT”). These maps may be created from scratch using any Windows paint program, however it is best to scan in an existing site map. Commercial copy centers usually have scanners that can handle larger drawing sizes.

If an AutoCad file is available, have AutoCad export a bitmap for the best looking maps that require the least work to make presentable. If the scale of the exported map is too large or too small, re-export the map at the corrected scale rather than scaling the map in a graphic editor. Scaling a bitmap file directly will produce a file that will require a significant amount of manual effort to make presentable.

Save the scanned image as a Windows bitmap file (.BMP) with 256 colors (8 bit color). High Color (16 bit) or True Color (24 bit) can also be used, but the file sizes will be much larger and the maps will be slower to load and may require more system RAM. It should be scaled so that the entire map file is at least 800 by 600 pixels (covering the entire Windows screen). The Security Escort software auto scrolls the map; therefore it is not a problem if the map is larger than the screen. The map should not be too large. There should be enough area of the map on the screen when an alarm is shown, so there is no question where in the facility the alarm is located from a quick review of the map. A good rule-of-thumb is 100 pixels would represent 15 m (50 ft) or greater.

Multiple map files

For a multi-story building, the maps for each floor must have the same resolution. Each map must be vertically aligned with all the floors above and below it. Therefore the maps will have the same origin (0,0 = upper left corner). Typically, you would do the map for the ground floor, then make the maps for the other floors by editing copies of the ground floor map.

Where transponders from multiple systems are reporting into the same computer, the map(s) for each system is separate and assigned unique map numbers, from the other maps on that same computer. The origin for the maps for each system is 0,0 = upper left corner. Therefore, the location of the receivers in the transponder database will only consider this system’s map without respect to the maps for any other systems being handled by the same computer.

The maps must be named MAP0.EDB, MAP1.EDB through MAP99.EDB. Where MAP0.EDB is the default map file, usually the ground floor. The Security Escort software shows the default map if there are no other events being processed at a given time.

Assign the desired map number to an area or point in the **Transponder Database**. Assign the map for a fixed location transmitter in the **Subscriber Database Advanced** dialog.

Subscriber images

Display subscriber images. This software does not capture the subscriber images; it displays images that were previously captured by some other means. The subscriber image can be captured using a digital camera, video capture board and so on. The source of the image is not critical. We have not identified, nor do we require a specific manufacturer of the image capture equipment. The images must be saved individually in JPG format. The images should not be larger that 160 pixels wide and 160 pixels high. If they are, they are scaled and therefore they may loose image quality. Under **Setup** > **System Preferences** dialog, the path to the images is set in subscriber image file path (default location of the images is "C:\ESCORT

\IMAGES", but they can be located anywhere). The three-character file extension of the image files is set in **Extension** (default is “JPG”). Subscriber images can also be saved in Windows bitmap (“BMP”); however, this format requires significantly more disk storage.

Only when the display is set to 640 by 480 (not recommended) the images display on top of the map and the **Scaling %** (10 to 200) controls the size of the image (try different settings to control the image size in the alarm screen). Under **Files > Subscriber Database** dialog, select the desired subscriber and click the **[Edit data]** button. The image file is the name of file that has this subscriber’s image. For example, if the subscriber’s image is stored with the file name “Image1.jpg”, enter “**Image1”** in this box. You should have a minimum of 1 MB video card to display subscriber’s images. Go to the Windows **Start** button. Select **Settings** > **Control Panel** > **Display**. Click the **Settings** tab. In the **Color palette** control you can select 256 color, High Color (16 bit) or True Color (24 bit). Set the system to High Color or True Color (256 color is likely to produce undesirable results). When in doubt, set to High Color. In the same dialog window, **Desktop area** can be set to 640 by 480, 800 by 600, or 1024 by 768 pixels. When the display is set to 640 by 480 (not recommended), the images are displayed on top of the map and therefore limit how much of the map displays. The 1024 by 768 setting may require too much memory for most video cards and show more of the map, decreasing the size of the map details. Most video cards can be set to 800 by 600 and when in doubt this setting should be selected. If you cannot choose these settings, your video card or monitor setting may be incorrect, refer to the system documentation to correct.

6 Security Escort pager setup

With version 1.10 and higher, Security Escort supports:

- Up to 256 individual alphanumeric pagers; grouped into 99 groups of eight.
- Both dial up and local serial port connected paging systems, in the same system, at the same time.
- Service pages that can activate a group of eight service pagers in addition to a single pager.
- Alarm pages that can activate a group of eight alarm pagers in addition to a single pager. All alarms located in an alarm area can page an additional group of eight pagers specific to that area.
- Manual pages sent to any individual pager or pager group.
- All paging system communication using the TAP or PET protocols. This is true for both the dial-up and local serial port connected paging systems. Currently there is no support for any other pager protocols.
- Pager message enhanced to be able to send alarm restore from workstation.

The system does not support numeric only or vibrate only pagers.

At this time, the only local paging system tested is TEKK model: PT-400 (Tekk Inc., 226 N. W. Parkway, Kansas City, MO, Phone (816) 746-1098, Fax (816) 746-1093).

Set the DIP switch for TAP Mode, 9600N81, Switch 6 off, all other switches on.

The pager ID to be used for each pager is the seven-digit CAP code that is on a label on the back of the pager (such as 0991001). A three-digit code must be appended to the end of the CAP code. For example, 0991001ERF where E is the Message Encoding Type, R is the RF data rate, and F is the Function Code.

Message Encoding Type (E) must be a “1” for alphanumeric coding.

RF data rate (R) is “5” for 512 BPS, “1” for 1200 BPS, or “2” for 2400 BPS. Many systems use 512 BPS for more reliable transmissions.

Function Code (F) may be set to one through four for a specific function code or zero for the default (recommend the Function Code be set to zero).

For an alphanumeric pager communicating at 512 BPS, the pager ID in our example is 0991001150.

For dial-up paging systems, the paging company assigns the phone number and Pager ID. Typically, the pager ID is the last seven digits dialed to access the pager from a phone.

Service pages page the members of the service group first, followed by the single service pager.

Alarm pages page the members of the alarm area paging group first (if any), followed by the alarm group, and finally the single alarm pager.

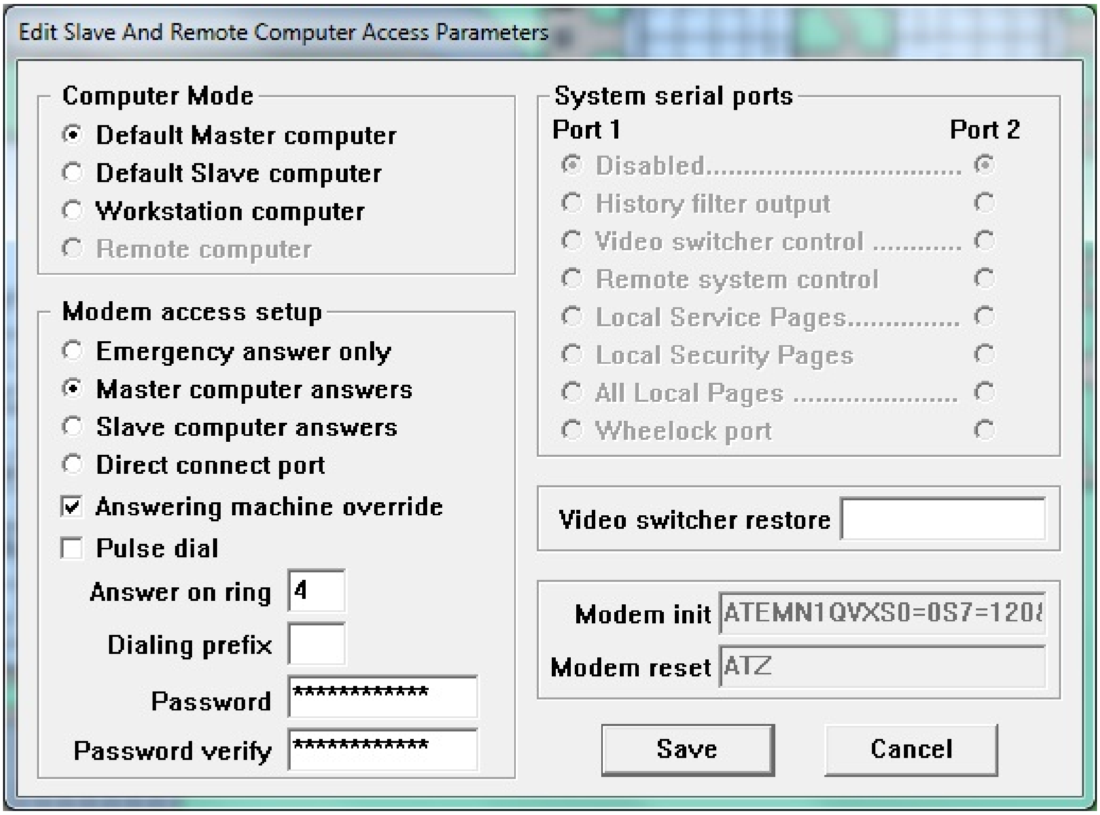
6.1 Dial-up paging modem setup

All dial-up pager access is through the modem. The baud rate set up of the modem port in the **Remote comm port setup** dialog under the **Setup** menu is for remote access to the Security Escort System, and not for pager dial-up access. Leave this baud rate at the correct setting for remote access.

6.2 Local paging setup

The local paging system is accessed through a system serial port. This can be configured using the **Remote comm port setup** dialog under the **Setup menu**. Use the **System Serial Port 1 or 2**. Also, configure the baud rate to match the local paging system (typically 9600 baud).

In the **Remote Setup** dialog, assign **System Serial Port 1 or 2** as the destination for **Local Service Pages**, **Local Security Pages**, or **All Local Pages**.



Edit Slave And Remote Computer Access Parameters

Computer Mode
- ● Default Master computer
- ○ Default Slave computer
- ○ Workstation computer
- ○ Remote computer

Modem access setup
- ○ Emergency answer only
- ● Master computer answers
- ○ Slave computer answers
- ○ Direct connect port
- ☑ Answering machine override
- □ Pulse dial

Answer on ring: 4

Dialing prefix:

Password: ************

Password verify: ************

System serial ports

Port 1		Port 2
●	Disabled................................	●
○	History filter output	○
○	Video switcher control	○
○	Remote system control	○
○	Local Service Pages..............	○
○	Local Security Pages	○
○	All Local Pages	○
○	Wheelock port	○

Video switcher restore:

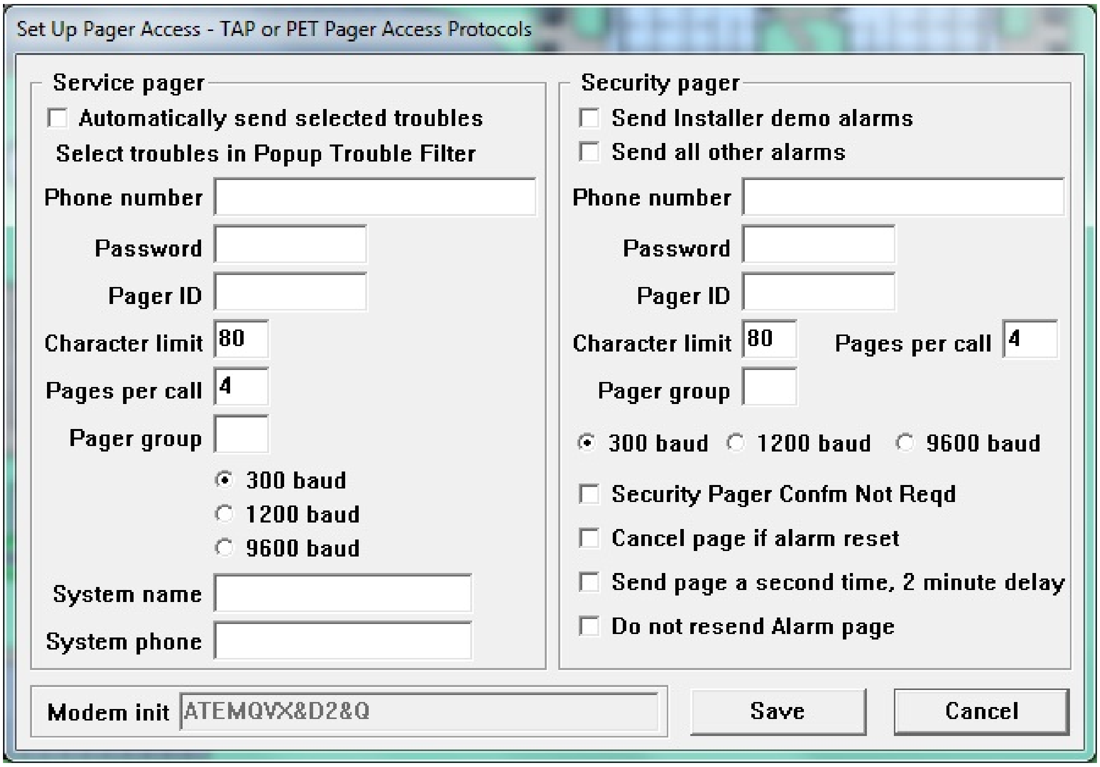
Modem init: ATEMN1QVXS0=0S7=120

Modem reset: ATZ

Figure 6.1: Remote Setup Dialog

6.3 Service and security (alarm) pager setup

Pager access is set up in the **Pager setup** dialog under the **Setup menu**. Refer to the **Pager setup** dialog for details that are not covered here.



Set Up Pager Access - TAP or PET Pager Access Protocols

Service pager

□ Automatically send selected troubles

Select troubles in Popup Trouble Filter

Phone number:

Password:

Pager ID:

Character limit: 80

Pages per call: 4

Pager group:

● 300 baud
○ 1200 baud
○ 9600 baud

System name:

System phone:

Security pager

□ Send Installer demo alarms

□ Send all other alarms

Phone number:

Password:

Pager ID:

Character limit: 80 Pages per call: 4

Pager group:

● 300 baud ○ 1200 baud ○ 9600 baud

□ Security Pager Confm Not Reqd

□ Cancel page if alarm reset

□ Send page a second time, 2 minute delay

□ Do not resend Alarm page

Modem init: ATEMQVX&D2&Q

Figure 6.2: Pager Setup Dialog

For both the service and security pagers, an individual pager (**Phone number**, **Password**, and **Pager ID**) can be assigned. The **Pager ID** is required for all individual pagers, dial-up and local. If the phone number and password are assigned, the page is sent over the modem connection. If the phone number and password fields are both blank, the page is routed to the local paging system. If you do not desire an individual pager, leave the **Phone number**, **Password**, and **Pager ID** fields blank.

Both the service and security pagers also support paging groups. If a group number is programmed in the **Pager group** field, all the members of that group are paged for every service or alarm page.

If service or alarm pages are enabled, either the paging group or individual pager must be filled in. They may both be filled in if desired.

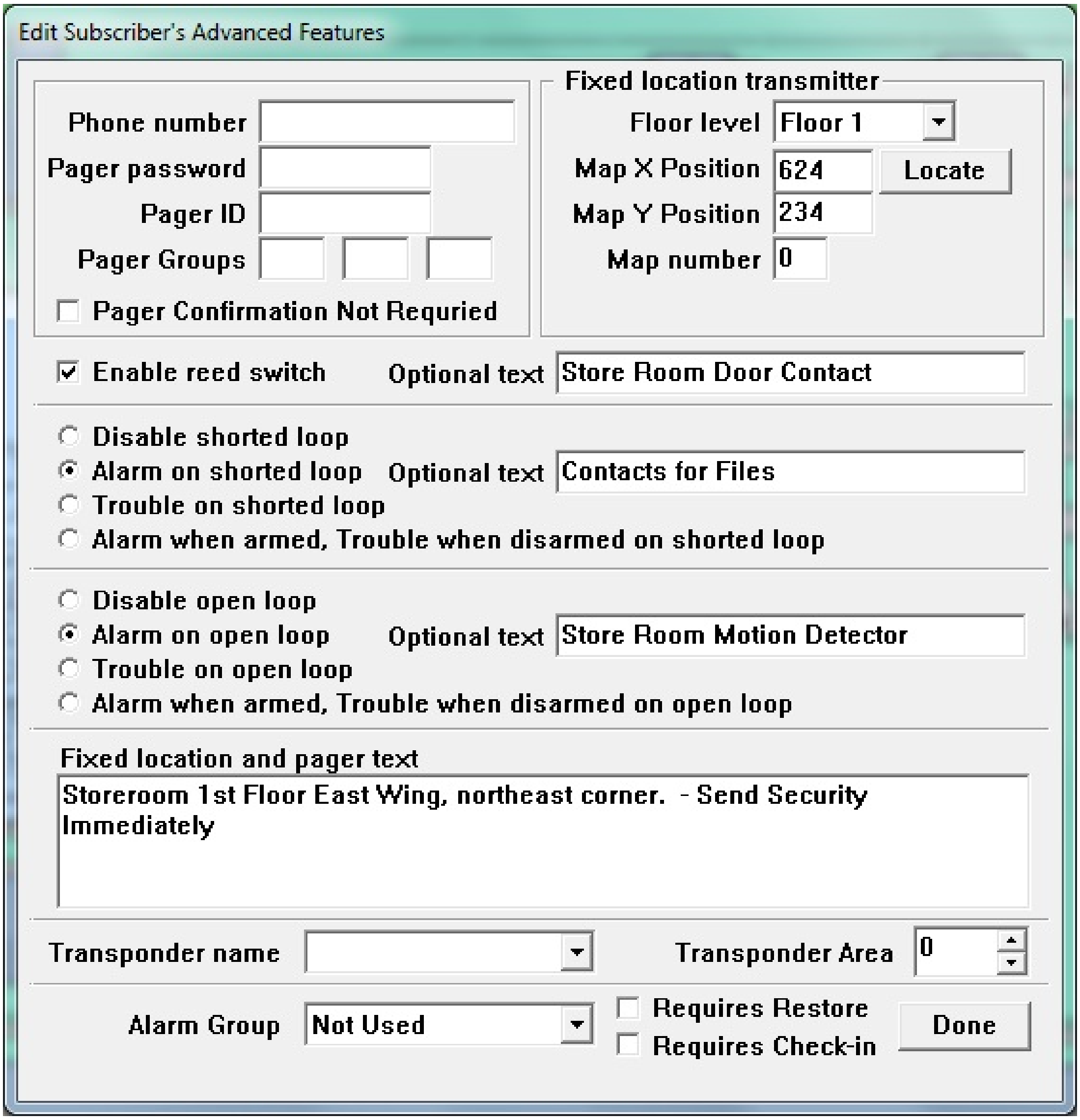
The baud rate assignments in this dialog affect only the dial-up paging access through the modem (get the desired baud rate from the paging company). These baud rate selections have no effect on local paging systems or remote system access. Remember that dial-up pages may be routed to different paging companies and they may require different baud rates. Set the baud rate to the highest baud rate common to all of the paging companies to be accessed.

The **Character limit** (characters per page), **Pages per call** affect all pages of the indicated type (local and dial-up). These fields must be set to the lowest setting for any of the routes that may be used. Remember that dial-up pages may be routed to different paging companies and they may have different restrictions.

6.4 Subscriber (individual) pager setup

In the **Subscriber Database**, select the record for the desired individual. Click the **[Edit Data]** button, followed by the **[Advanced]** button.

The **Pager ID** is required for all individual pagers dial-up and local. If the **Phone number** and **Pager password** are assigned, the page is sent over the modem connection. If the **Phone number** and **Pager password** fields are blank, the page is routed to the local paging system. If you do not desire this individual to have pager support, leave the **Phone number**, **Pager password**, and **Pager ID** fields blank.



Edit Subscriber's Advanced Features

Phone number:
Pager password:
Pager ID:
Pager Groups:
□ Pager Confirmation Not Requried

Fixed location transmitter
Floor level: Floor 1
Map X Position: 624
Map Y Position: 234
Map number: 0

☑ Enable reed switch — Optional text: Store Room Door Contact

○ Disable shorted loop
● Alarm on shorted loop — Optional text: Contacts for Files
○ Trouble on shorted loop
○ Alarm when armed, Trouble when disarmed on shorted loop

○ Disable open loop
● Alarm on open loop — Optional text: Store Room Motion Detector
○ Trouble on open loop
○ Alarm when armed, Trouble when disarmed on open loop

Fixed location and pager text: Storeroom 1st Floor East Wing, northeast corner. - Send Security Immediately

Transponder name:
Transponder Area: 0

Alarm Group: Not Used
□ Requires Restore
□ Requires Check-in

Figure 6.3: Subscriber Database Advanced Dialog

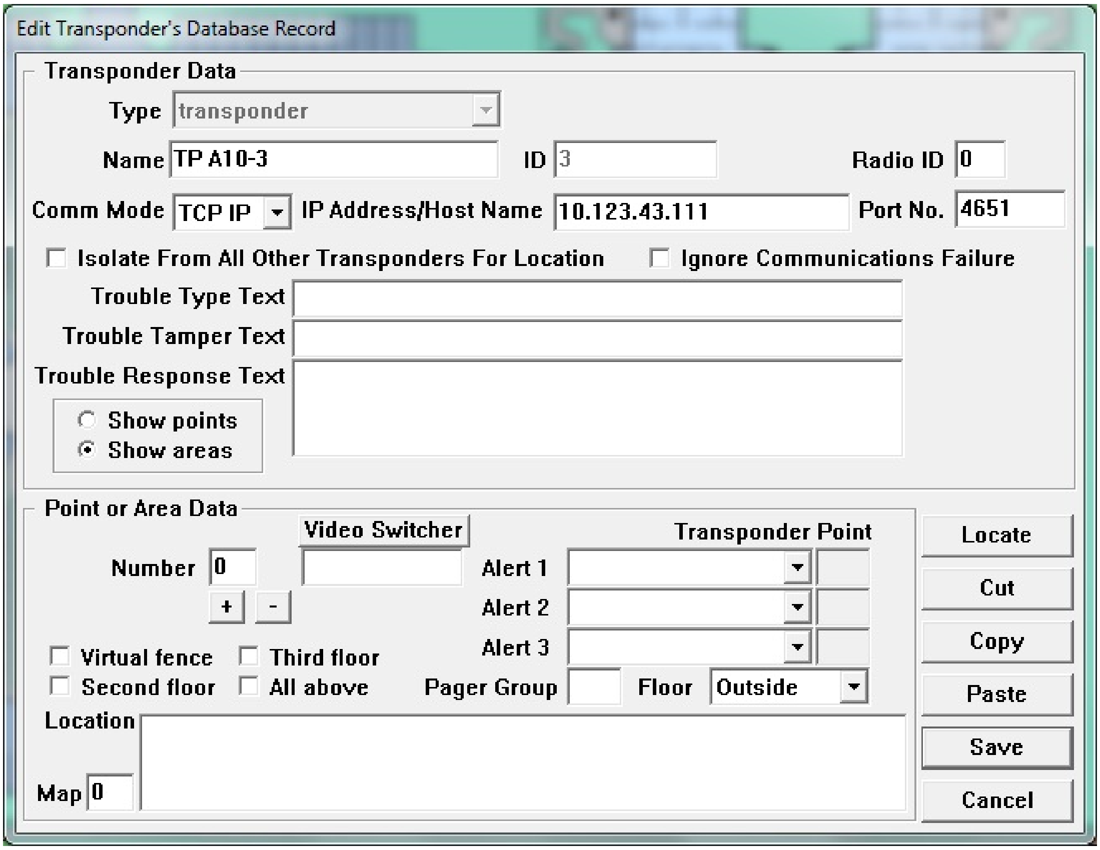
If the pager information is entered, this individual may be assigned to three paging groups. Each group accepts eight members maximum. Remember, it takes time to communicate with a paging service; therefore, only add members to a group if they need to be there. Otherwise, you may slow the paging report to people that must respond.

Notice!

A **Pager Group** may contain members accessed by the local paging system and members that require dial-up access. Dial-up access typically takes much longer and it may slow pages to the local paging system.

6.5 Alarm area setup

In the **Transponder Database** under the **File** menu, select the transponder where the alarm area is to be programmed in. Click the **[Edit Data]** button, followed by **Show areas** radio button and select the desired area.



Edit Transponder's Database Record

Transponder Data

Type: transponder

Name: TP A10-3 ID: 3 Radio ID: 0

Comm Mode: TCP IP IP Address/Host Name: 10.123.43.111 Port No.: 4651

□ Isolate From All Other Transponders For Location □ Ignore Communications Failure

Trouble Type Text

Trouble Tamper Text

Trouble Response Text

○ Show points
● Show areas

Point or Area Data

Number: 0 Video Switcher

Alert 1

Alert 2

Alert 3

□ Virtual fence □ Third floor
□ Second floor □ All above

Pager Group Floor: Outside

Location

Map: 0

Figure 6.4: Transponder Area Edit Dialog

Number Each transponder can have up to 80 areas defined in them (prior to version 2.04 of the software, only 40 areas could be defined). This area number range from 0 to 79. Use the **[Locate]** button to define the area graphically on the map.

Video Switcher Selects a system serial port that is programmed in the **Remote Setup** dialog. The purpose is to display the area, where the alarm is most likely located, on the CCTV monitors near the Central Console. The string would activate a macro in the video switcher that selects the appropriate camera, and controls any required zoom and tilt actions. Up to 40 characters may be entered. Control characters may be entered as "^A" for control A.

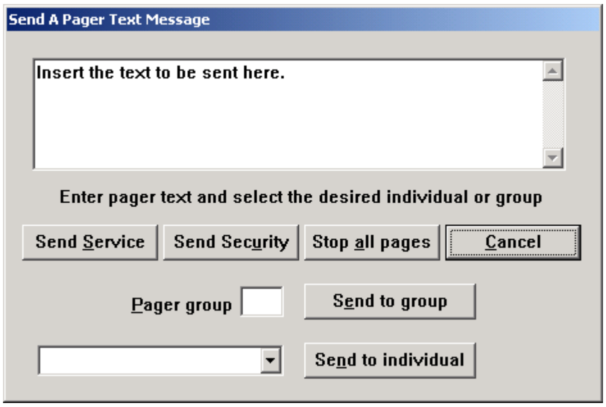
Pager Group This **Pager Group** field may be programmed with a pager group that is paged if the alarm location is determined to be in this area. This pager group will be the first group paged to allow quick response by those individuals charged with responding to an alarm in this area. Each area may be assigned a pager group that can be the same or different from other alarm areas.
The default alarm **Pager group** defined in the **Pager Setup** dialog will also be paged after the pager group is assigned to an area. If a pager group is not assigned to an area or the alarm location is not within a defined area, then only the default pager group will be paged.

Floor Determines the floor number that this area is defined for. The areas on floors above and below this one may be defined differently. In order for an area to be selected when an alarm is received, the location determined by the Central Console must be located within the defined area, and it must be located on the designated floor.

Virtual Fence Area If this checkbox is checked, this area will not be used for normal alarm area location. This area will only be used to define a “Virtual” fence. Specific transmitters in the **Subscriber Database** can reference this transponder and area. When they reference this area, and the system locates the transmitter position outside the area, a wandering (“Virtual” fence) alarm will be generated. This alerts the operator and shows the position of the transmitter.

6.6 Manual pages

Allows manually entered messages to be sent to the service or security pagers. Service and security pagers are configured in the **Pager setup** dialog. Individuals and group pager assignments are configured in the **Subscriber Database**.



Insert the text to be sent here.

Enter pager text and select the desired individual or group

Figure 6.5: Send Pager Message Dialog

Insert the text to be sent here. Enter the text to be sent to the pagers in the large text box at the top of the dialog.

[Send Service] Causes the entered message to be sent to the service pager and service pager group.

[Send Security] Causes the entered message to be sent to the security pager and security pager group.

[Stop all pages] Causes all pages currently queued (automatic or manual) to be aborted and deleted. Use with caution.

Pager group To send a page to all members of a group, enter the pager group number here (1 to 99).

[Send to group] Click this button to send the text entered to the indicated pager group.

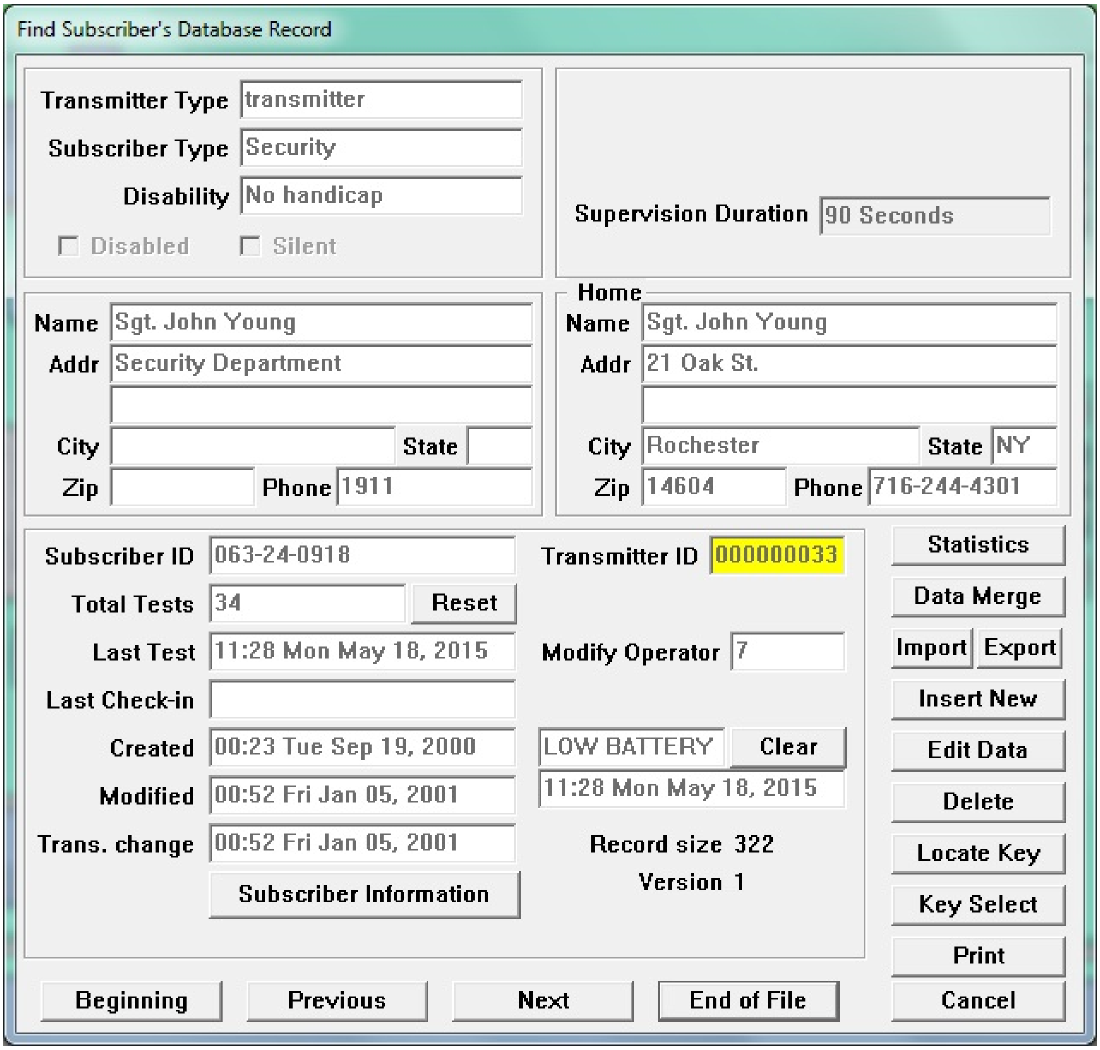
[Send to Individual] Click this button to send the text entered to the individual that is selected from the drop down list.

[Cancel] Cancel and close this dialog window..

7 Maintenance

7.1 Exporting, importing and merging the Subscriber Database

The following sections describe the steps to export, import and merge data from and into the **Subscriber Database**. The file formats for the tasks are included in detail.



Find Subscriber's Database Record

Transmitter Type: transmitter
Subscriber Type: Security
Disability: No handicap
□ Disabled □ Silent
Supervision Duration: 90 Seconds

Name: Sgt. John Young
Addr: Security Department
City: State:
Zip: Phone: 1911

Home
Name: Sgt. John Young
Addr: 21 Oak St.
City: Rochester State: NY
Zip: 14604 Phone: 716-244-4301

Subscriber ID: 063-24-0918
Transmitter ID: 000000033
Total Tests: 34
Last Test: 11:28 Mon May 18, 2015
Modify Operator: 7
Last Check-in:
Created: 00:23 Tue Sep 19, 2000
Modified: 00:52 Fri Jan 05, 2001
Trans. change: 00:52 Fri Jan 05, 2001
LOW BATTERY
11:28 Mon May 18, 2015
Record size 322
Version 1

Figure 7.1: Find Subscriber's Database Record Dialog

7.1.1 File format of "TABMERGE.DAT" / “TABMERGE_EXPORT.DAT”

The file of data record entries used for export, import and merge must be in tab delimited text format. For data merge and import, It must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”. For export functionality, the exported file is named as “TABMERGE_EXPORT.DAT”. Both file formats are the same.

The data fields must be in the following order, delimited by the horizontal tab character (decimal 8) and the record must be terminated with a carriage return (decimal 13). If a data field has no data, just store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters.

Data fields in required order	**Excel Column**	**Restrictions**
Subscriber Name	A	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Subscriber ID	B	This field may be up to 12 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.
Here Phone Number	C	This field may be up to 16 characters. This field may contain only numeric, ‘#’, ‘*’, ‘(‘, ‘)’, comma and the dash ASCII characters.
Here Address 1	D	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Here Address 2	E	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Here City	F	This field may be up to 20 characters. This field may contain any printable ASCII character except the ‘?’.
Here State	G	This field may be up to 3 characters. This field may contain only ALPHA ASCII characters.
Here Zip	H	This field may be up to 10 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.
Away Phone Number	I	This field may be up to 16 characters. This field may contain only numeric, ‘#’, ‘*’, ‘(‘, ‘)’, comma and the dash ASCII characters.
Away Address 1	J	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Away Address 2	K	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Away City	L	This field may be up to 20 characters. This field may contain any printable ASCII character except the ‘?’.
Away State	M	This field may be up to 3 characters. This field may contain only ALPHA ASCII characters.
Away Zip	N	This field may be up to 10 characters. This field may contain only ALPHA, numeric and the dash ASCII characters.

Data fields in required order	Excel Column	Restrictions
Supplemental Text Field 1	O	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’.
Supplemental Text Field 2	P	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’.
Supplemental Text Field 3	Q	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’.
Supplemental Text Field 4	R	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’.
Pager Phone Number	S	This field may be up to 16 characters. This field may contain only numeric, ‘#’, ‘*’, ‘(‘, ‘)’, comma and the dash ASCII characters.
Pager Password	T	This field may be up to 6 characters. This field may contain only numeric, and ALPHA ASCII characters.
Pager Pager ID	U	This field may be up to 10 characters. This field may contain only numeric ASCII characters.
Subscriber Type	V	"0 Unclassified", "1 Commuter", "2 Faculty", "3 Resident", "4 Security", "5 Staff", "6 Installer", "7 Out of Service", "8 Watchman", "9 Visitor", "10 Point type", "11 Acknowledgement". This field should contain only numeric ASCII characters.
Handicapped Type	W	"0 No handicap", "1 Blind", "2 Deaf", "3 Handicapped", "4 Wheel chair". This field should contain only numeric ASCII characters.
Transmitter ID	X	This field may be up to 9 characters. This field should contain only numeric ASCII characters.
Away Name	Y	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’.
Image Filename	Z	This field may be up to 30 characters. This field may contain any printable ASCII character that is valid for a file name.
Height Feet	AA	0-7, This field should contain only numeric ASCII characters.
Height Inches	AB	0-11, This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Build Code	AC	"0 Medium", "1 Slim", "2 Large". This field should contain only numeric ASCII characters.
Hair Color	AD	"0 Brown", "1 Auburn", "2 Black", "3 Blond", "4 Brunet", "5 Grey", "6 Red". This field should contain only numeric ASCII characters.
Eye Color	AE	"0 Brown", "1 Blue", "2 Green", "3 Hazel", "4 Grey". This field should contain only numeric ASCII characters.
Pager Group A	AF	0-99, This field should contain only numeric ASCII characters.
Pager Group B	AG	0-99, This field should contain only numeric ASCII characters.
Pager Group C	AH	0-99, This field may contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Fixed Floor Level	AI	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Fixed Map X Location	AJ	This field may contain only numeric ASCII characters.
Fixed Map Y Location	AK	This field may contain only numeric ASCII characters.
Fixed Bitmap Number	AL	0-99 This field may contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Supervision Interval	AM	“0 None”, “1 is 90 Second Supervision”, “2 is 30 Second Supervision”, “3 is 1 Hour Supervision. This field may contain only numeric ASCII characters.
Alarm Group	AN	0-99, This field may contain only numeric ASCII characters.
Shorted Loop	AO	This field may contain only numeric ASCII characters.
Open Loop	AP	This field may contain only numeric ASCII characters.
Status	AQ	Encoded value. Do not change.
Enable Magnetic Reed	AR	This field may contain only numeric ASCII characters.
Fixed Location Text	AS	This field may be up to 254 characters. This field may contain any printable ASCII character except the ‘?’
Magnetic Reed Text	AT	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Shorted Loop Text	AU	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Open Loop Text	AV	This field may be up to 30 characters. This field may contain any printable ASCII character except the ‘?’
Status Flags	AW	Encoded value. Do not change.
Modify Op	AX	0-30000, This field may contain only numeric ASCII characters.
Test Time	AY	Encoded 32-bit time value. Do not change.
Last Transmitter Change	AZ	Encoded 32-bit time value. Do not change.
Spare Date	BA	Encoded 32-bit time value. Do not change.
Last Fail To Test Letter	BB	Encoded 32-bit time value. Do not change.
Created	BC	Encoded 32-bit time value. Do not change.
Modified	BD	Encoded 32-bit time value. Do not change.
Low Battery	BE	Encoded 32-bit time value. Do not change.
Spare2	BF	This field should be blank.
Spare3	BG	This field should be blank.

7.1.2 Exporting the Subscriber Database

This section describes the information required to export data from the **Subscriber Database**.

Notice!

There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

To import or merge data from the import/merge file, you will need to format the data and columns according to a specific format. To simplify the preparation, it is recommended that you perform the export function first, so that you can use the exported file as your template for your data import/merge. You will need to rename the file from “TABMERGE_EXPORT.DAT” to “TABMERGE.DAT” accordingly.

Only users or operators who are assigned the minimum security level of “View Subscribers” are able to view the **Subscriber Database**. Go to menu **File >Subscriber Database** dialog, and click the **[Export]** button.

Notice!

Important! The export operation does not change the existing records in **Subscriber Database**. However, be mindful that every time you perform the export function (clicking the **[Export]** button), the operation will overwrite the “TABMERGE_EXPORT.DAT” file.

Be patient, as it may take a while, and watch for the disk activity to stop. If the export is successful, a confirmation dialog appears. You will find the “TABMERGE_EXPORT.DAT” file in the Security Escort folder (typically “C:\ESCORT”).

7.1.3 Importing the Subscriber Database

This section describes the information required to import data into the **Subscriber Database**.

Notice!

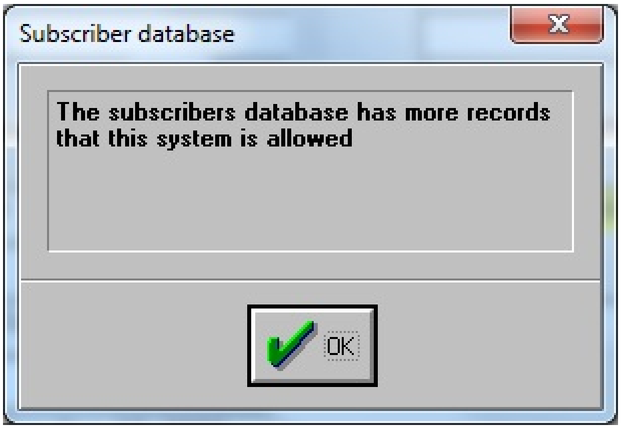
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

Proceeding with the import operation will delete all existing records in **Subscriber Database**. The record entries in “TABMERGE.DAT” are then imported to the **Subscriber Database,** validated and sorted by the **Subscriber ID**.

The number of record entries that is imported is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the import, a pop-up message appears to inform the user.

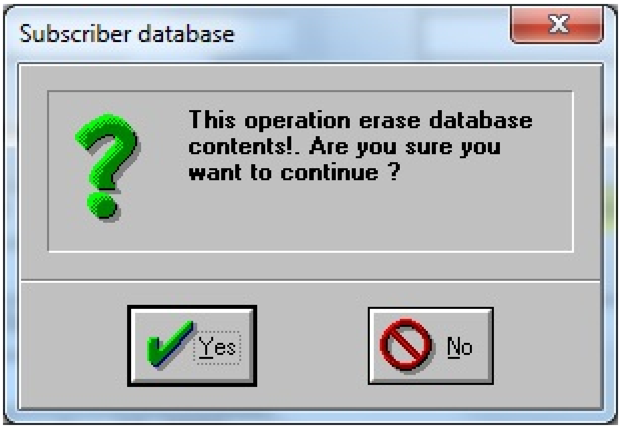


Subscriber database

The subscribers database has more records that this system is allowed

The **[Import]** button is only visible to users or operators who are assigned the minimum security level of “Install”, and if the file to import is named accordingly in the correct folder. The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”.

After preparing the “TABMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Subscriber Database** dialog, and click the **[Import]** button. A popup dialog appears asking for confirmation to proceed with the import or to abort the operation.



Subscriber database

This operation erase database contents!. Are you sure you want to continue ?

Figure 7.2: Subscriber Database Import Confirmation Dialog

Click the **[Yes]** button to continue. Otherwise, click the **[No]** button to abort. Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a pop-up confirmation message appears. It is a good idea to remove the “TABMERGE.DAT” file, to disable the import feature (the **[Import]** button becomes invisible). If the data is not imported successful, a pop-up error message appears. The error message will indicate the likely issue causing the import to fail.

7.1.4 Merging the Subscriber Database

This section describes the information required to merge data into the **Subscriber Database**.

Notice!

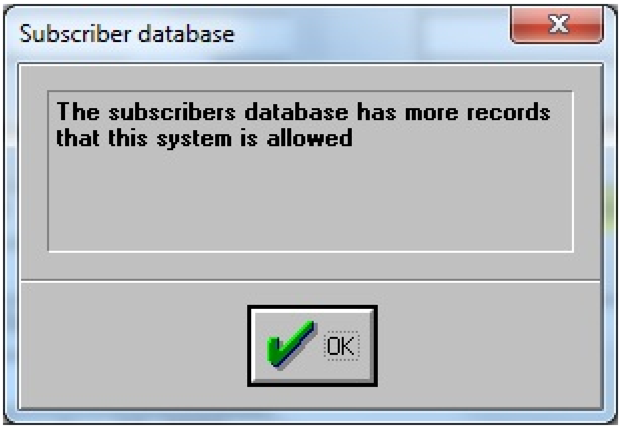
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Subscriber Database** from the backup.

Notice!

Important!

The record entries in the “TABMERGE.DAT” are merged with existing records in the **Subscriber Database**. If the **Subscriber ID** field in the file matches a record in the **Subscriber Database**, the existing record will be merged with the corresponding record entry in the file. Unmatched records will be inserted into the **Subscriber Database** as new records.

The total number of records is subject to the number of subscribers allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the merge, a pop-up message appears to inform the user.



Subscriber database

The subscribers database has more records that this system is allowed

The **[Data Merge]** button is only visible to users or operators who are assigned the minimum security level of “Install”, and if the file to import is named accordingly in the correct folder.

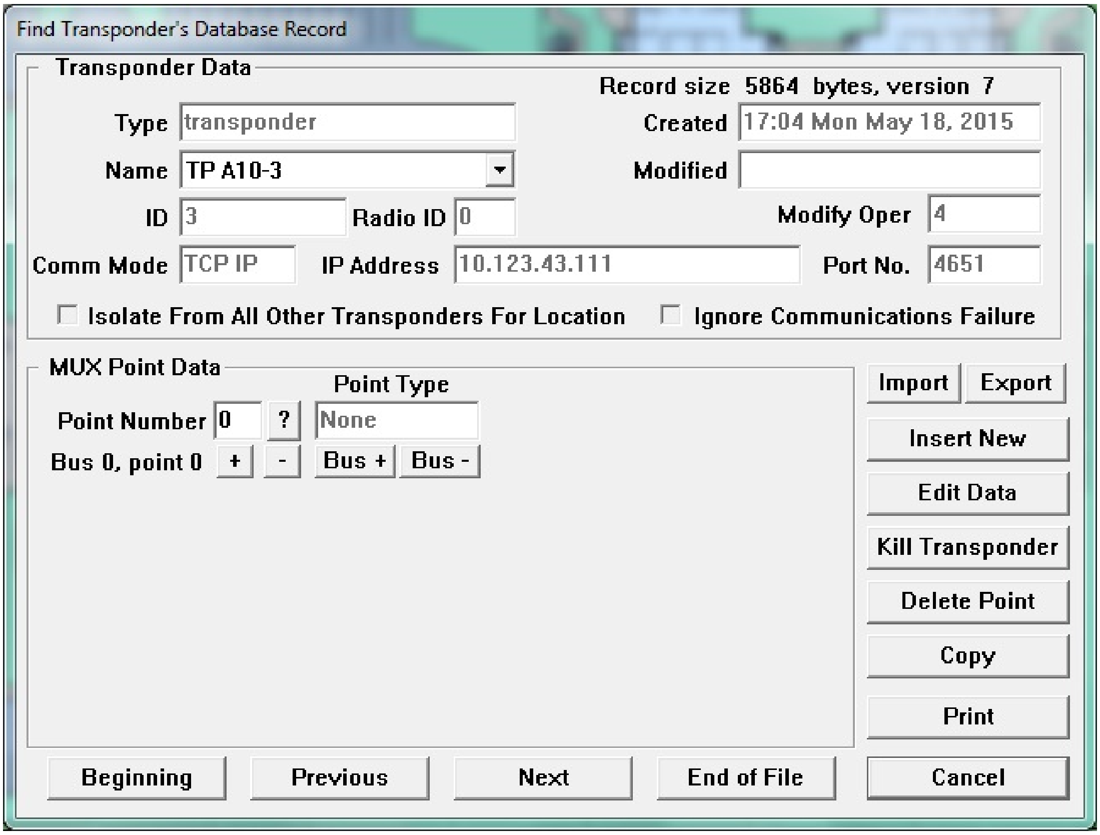
The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TABMERGE.DAT”.

After preparing the “TABMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Subscriber Database** dialog, and click the **[Data Merge]** button.

Be patient, as it may take a while, and watch for the disk activity to stop. If the data is merged successfully, a pop-up confirmation message appears. It is a good idea to remove the “TABMERGE.DAT” file, to disable the merge feature (the **[Data Merge]** button becomes invisible).

7.2 Exporting and importing the Transponder Database

The following sections describe the steps to export and import data from and into the **Transponder Database**. The file formats for the tasks are included in detail.



Find Transponder's Database Record

Transponder Data

Record size 5864 bytes, version 7

Type: transponder

Created: 17:04 Mon May 18, 2015

Name: TP A10-3

Modified:

ID: 3

Radio ID: 0

Modify Oper: 4

Comm Mode: TCP IP

IP Address: 10.123.43.111

Port No.: 4651

□ Isolate From All Other Transponders For Location

□ Ignore Communications Failure

MUX Point Data

Point Number: 0

Point Type: None

Bus 0, point 0

Figure 7.3: Find Transponder's Database Record Dialog

7.2.1 File format of "TRANSMERGE.DAT" / "TRANSMERGE_EXPORT.DAT"

The file of data record entries must be in tab delimited text format. For import functionality, It must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TRANSMERGE.DAT”. For export functionality, the exported file is named as “TRANSMERGE_EXPORT.DAT”. Both file formats are the same.

The data fields must be in the following order, delimited by the horizontal tab character (decimal 8) and the record must be terminated with a carriage return (decimal 13). If a data field has no data, just store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters.

Notice!

Area data of the transponders is not supported. Only point data of the transponders is used for the export and import functionalities.

Data fields in required order	Excel Column	Restrictions
Transponder ID	A	1-255. This field should contain only numeric ASCII characters.
Coordinator ID	B	Reserved for future use, this field should contain only the numeric 0.

Data fields in required order	Excel Column	Restrictions
Transponder Name	C	This field may be up to 24 characters. This field may contain any printable ASCII character except the ‘?’
IP Connected	D	"0 RS232", "1 TCP IP". This field should contain only numeric ASCII characters.
Coordinator	E	0. Reserved for future use, this field should contain only the numeric “0”.
IP Address	F	This field is blank if **IP Connected** is 0 (RS232). This field should contain a valid IP address if **IP Connected** is 1 (TCP .IP).
Port Number	G	This field is blank if **IP Connected** is 0 (RS232). This field should contain only numeric ASCII characters, 1-65535.
Comm Port Index	H	This field used only if **IP Connected** is 0 (TCP IP). “0 A”, “1 B”, “2 C”, “3 D”, “4 E”, “5 F”, “6 G”, “7 H”, “8 I”, “9 J”, “10 K”, “11 L”
Ignore Communications Failure	I	This field is 0 if this is not selected. This field is 1 if this is selected. This field should contain only numeric ASCII characters.
Isolate For Location	J	This field is 0 if this is not selected. This field is 1 if this is selected. This field should contain only numeric ASCII characters.
Trouble Text	K	This field may be up to 40 characters. This field may contain any printable ASCII character except the ‘?’.
Tamper Text	L	This field may be up to 40 characters. This field may contain any printable ASCII character except the ‘?’.
Trouble Response	M	This field may be up to 135 characters. This field may contain any printable ASCII character except the ‘?’
Point Number 0	N	This field must be 0 (the point number). This field should contain only numeric ASCII characters.
Point Type	O	“0 receiver”, “1 Alert unit”, “2 Virtual”, “7 None”. This field should contain only numeric ASCII characters.
Algorithm Number	P	“0 Default”, “1 Classic”. “2 Linear”, “3 Low”, “4 Medium”, “5 Strong”. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Floor	Q	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Alert Unit 1	R	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 1 Point	S	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 2	T	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	U	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	V	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	W	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	X	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	Y	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	Z	This field may be up to 100 characters. This field may contain any printable ASCII character except the ‘?’.
Map X Position	AA	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	AB	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	AC	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	AD	0-99. This field should contain only numeric ASCII characters.
Point Number 1	AE	This field must be 1 (the point number). This field should contain only numeric ASCII characters.
Point Type	AF	“0 receiver”, “1 Alert unit”, “2 Virtual”, “7 None”. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Algorithm Number	AG	“0 Default”, “1 Classic”. “2 Linear”, “3 Low”, “4 Medium”, “5 Strong”. This field should contain only numeric ASCII characters.
Floor	AH	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.
Alert Unit 1	AI	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 1 Point	AJ	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 2	AK	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	AL	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	AM	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	AN	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	AO	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	AP	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	AQ	This field may be up to 100 characters. This field may contain any printable ASCII character except the ‘?’.
Map X Position	AR	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	AS	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	AT	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	AU	0-99. This field should contain only numeric ASCII characters.
. . .		

Data fields in required order	**Excel Column**	**Restrictions**
Point Number 63	AOS	This field must be 63 (the point number). This field should contain only numeric ASCII characters.
Point Type	AOT	“0 receiver”, “1 Alert unit”, “2 Virtual”, “7 None”. This field should contain only numeric ASCII characters.
Algorithm Number	AOU	“0 Default”, “1 Classic”. “2 Linear”, “3 Low”, “4 Medium”, “5 Strong”. This field should contain only numeric ASCII characters.
Floor	AOV	"0 Basement5", "1 Basement4", "2 Basement3", "3 Basement2", "4 Basement1", "5 Tunnel", "6 Basement ", "7 Ground","8 Outside", "9 Floor 1", "10 Floor 2", "11 Floor 3", "12 Floor 4", "13 Floor 5", "14 Floor 6", "15 Floor 7", "16 Floor 8", "17 Floor 9", "18 Floor 10", "19 Floor 11", "20 Floor 12", "21 Floor 13", "22 Floor 14", "23 Floor 15", "24 Floor 16", "25 Floor 17", "26 Floor 18", "27 Floor 19", "28 Floor 20", "29 Floor 21", "30 Floor 22", "31 Floor 23", "32 Floor 24", "33 Floor 25", "34 Floor 26", "35 Floor 27", "36 Floor 28", "37 Floor 29", "38 Floor 30", "39 Floor 31", "40 Floor 32", "41 Floor 33", "42 Floor 34", "43 Floor 35", "44 Floor 36", "45 Floor 37", "46 Floor 38", "47 Floor 39", “48 Floor 40”, “49 Floor 41”, “50 Floor 42”, “51 Floor 43”, “52 Floor 44”, “53 Floor 45”, “54 Floor 46”, “55 Floor 47”, “56 Floor 48”, “57 Floor 49”, “58 Floor 50”, “59 Floor 51”, “60 Floor 52”, “61 Floor 53”, “62 Floor 54”, “63 Floor 55”, “64 Floor 56”, “65 Floor 57”, “66 Floor 58”, “67 Floor 59”, “68 Floor 60”, “69 Floor 61”, “70 Floor 62”, “71 Floor 63”, “72 Floor 64”, “73 Floor 65”, “74 Floor 66”, “75 Floor 67”, “76 Floor 68”, “77 Floor 69”, “78 Floor 70”, “79 Floor 71”, “80 Floor 72”, “81 Floor 73”, “82 Floor 74”, “83 Floor 75”, “84 Floor 76”, “85 Floor 77”, “86 Floor 78”, “87 Floor 79”, “88 Floor 80”, “89 Floor 81”, “90 Floor 82”, “91 Floor 83”, “92 Floor 84”, “93 Floor 85”, “94 Floor 86”, “95 Floor 87”, “96 Floor 88”, “97 Floor 89”, “98 Floor 90”, “99 Floor 91”, “100 Floor 92”, “101 Floor 93”, “102 Floor 94”, “103 Floor 95”, “104 Floor 96”, “105 Floor 97”, “106 Floor 98”, “107 Floor 99”. This field should contain only numeric ASCII characters.

Data fields in required order	Excel Column	Restrictions
Alert Unit 1	AOW	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 1 Point	AOX	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 2	AOY	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 2 Point	AOZ	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit 3	APA	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit 3 Point	APB	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Alert Unit Test	APC	This field contains the Transponder ID of the alert unit. If this is not configured, this field is 0. This field should contain only numeric ASCII characters.
Alert Unit Test Point	APD	This field contains the alert unit point number. If this is not configured, this field is -1. This field should contain only numeric ASCII characters.
Point Location Text	APE	This field may be up to 100 characters. This field may contain any printable ASCII character except the ‘?’.
Map X Position	APF	X position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Map Y Position	APG	Y position of the point on the map. Default is 0. This field should contain only numeric ASCII characters.
Sensitivity Adjust	APH	0-99. This field should contain only numeric ASCII characters.
Bitmap Number	API	0-99. This field should contain only numeric ASCII characters.

7.2.2 Exporting the Transponder Database

This section describes the information required to export data from the **Transponder Database**.

Notice!

There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Transponder Database** from the backup.

To import data from the import file, you will need to format the data and columns according to a specific format. To simplify the preparation, it is recommended that you perform the export function first, so that you can use the exported file as your template for your data import. You will need to rename the file from “TRANSMERGE_EXPORT.DAT” to “TRANSMERGE.DAT” accordingly.

Only users or operators who are assigned the minimum security level of “Install” is able to view the **Transponder Database**. Go to menu **File > Transponder Database** dialog, and click the **[Export]** button.

Notice!

Important! The export operation does not change the existing records in **Transponder Database**. However, be mindful that every time you perform the export function (clicking the **[Export]** button), the operation will overwrite the “TRANSMERGE_EXPORT.DAT” file.

Be patient, as it may take a while, and watch for the disk activity to stop. If the export is successful, a confirmation dialog appears. You will find the “TRANSMERGE_EXPORT.DAT” file in the Security Escort folder (typically “C:\ESCORT”).

7.2.3 Importing the Transponder Database

This section describes the information required to import data into the **Transponder Database**.

Notice!

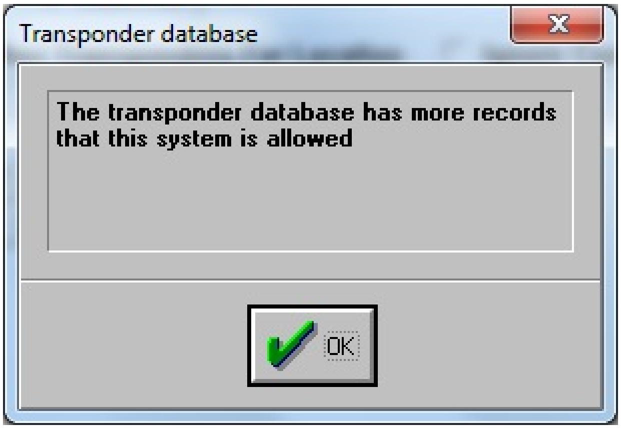
There is no way to undo the operations. Therefore, it is recommended to **perform a database backup** prior to starting the task. Upon completion of the task, verify the updated data before the new database is placed in service. If there are problems, restore the **Transponder Database** from the backup.

Notice!

Important!

Proceeding with the import operation will delete all existing records in **Transponder Database**. The record entries in “TRANSMERGE.DAT” are then imported to the **Transponder Database,** validated by the **Transponder ID**.

The number of record entries that is imported is subject to the number of transponders allowed for the purchased license. You can find this limit in the menu **About > About...** If this limit is reached during the import, a pop-up message appears to inform the user.

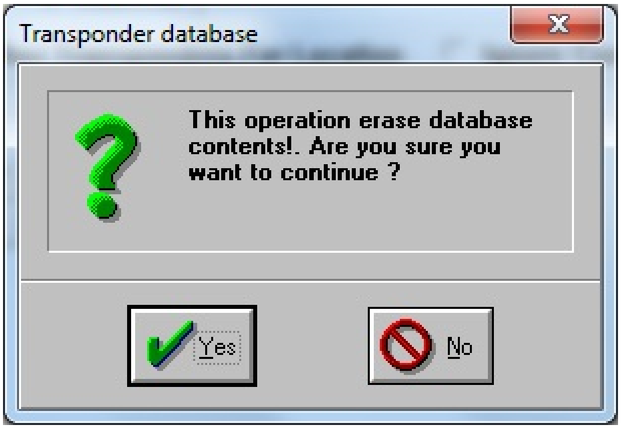


Transponder database

The transponder database has more records that this system is allowed

Only users or operators who are assigned the minimum security level of “Install” is able to view the **Transponder Database**. The file of data record entries must be placed in the Security Escort folder (typically “C:\ESCORT”) and named as “TRANSMERGE.DAT”.

After preparing the “TRANSMERGE.DAT” file in the Security Escort folder, start the Security Escort software. Go to menu **File > Transponder Database** dialog, and click the **[Import]** button. A popup dialog appears asking for confirmation to proceed with the import or to abort the operation.



Transponder database

This operation erase database contents!. Are you sure you want to continue ?

Figure 7.4: Transponder Database Import Dialog

Click the **[Yes]** button to continue. Otherwise, click the **[No]** button to abort. Be patient, as it may take a while, and watch for the disk activity to stop. If the data is imported successfully, a pop-up confirmation message appears. If the data is not imported successful, a pop-up error message appears. The error message will indicate the likely issue causing the import to fail.

7.3 System redundancy

The Security Escort system redundancy is operational as long as master and slave controllers are configured in a network setup. By default, master computer is the one controlling the devices. If the master computer is unavailable for some reasons, slave computer could take over the operation (automatically or manually). Once the master computer is back online, slave computer will hand over the control to the master computer. If both the master and slave computers are not available, the system is not operational. Devices will take control by themselves.

Notice!
In the event where the master computer is unavailable and the slave computer takes control of the devices, alarms will be reported on the slave computer. If the master computer becomes available again, it will try to take control of the devices.
However, if there are still **unacknowledged alarms** on the slave computer, the master computer will not succeed in taking control, as the alarms need to be acknowledged on the slave computer first. The master computer will try to take control of the devices continuously until the unacknowledged alarms on the slave computer are acknowledged accordingly.
During the acknowledgement process, the receiver's sounders and red LEDs may not be turned off properly. You may need to turn these off manually from menu **Setup > Receiver configuration**.

There are 2 types of redundancy:

1. Automatic redundancy – system will automatically determine which computer will be the main controller based on the online availability of the master and slave computers (not applicable for RS232 connections).
2. Manual redundancy – manually determine which computer (master or slave) will be the main controller.

7.3.1 Automatic redundancy

Automatic redundancy kicks in during the following circumstances:

1. Master computer information is not configured in slave computer – If the master computer's related information is not configured in the slave computer, the slave computer will consider the master computer as unavailable. As such, the control of devices will switch to the slave computer automatically.
2. Master computer not reachable from slave computer – If the master computer's related information is configured in the slave computer, but the slave computer is unable to connect to the master computer, the slave computer will keep attempting to connect for 10 consecutive times. If the slave computer is still unable to connect to the master computer, the control of devices will switch to the slave computer automatically.
3. Master computer not responding – The slave computer will send "heart beat" messages to the master computer every second. The master computer will acknowledge each "heart beat" messages to the slave computer. If the slave computer did not receive 6 continuous "heart beat" acknowledgements from the master computer, the slave computer will consider the master computer as unreachable. As such, the control of devices will switch to the slave computer automatically.

4. Master computer acknowledges “heart beat” message – The slave computer will send the “heart beat messages” continuously. Once the slave computer receives the “heart beat” acknowledgement from the master computer, the slave computer will consider the master computer as being back in operation. As such, the slave computer disconnects all the devices and requests the master computer to take control of the devices.

7.3.2 Manual redundancy

Manual redundancy is only applicable to the following circumstances:

1. RS232 connected to either master or slave computer – Switch the RS232 connection manually to the other computer.
2. Newly RS232 connected computer takes control – The newly RS232 connected computer will inform the other computer to lose their control. The other computer will disconnect all the devices. The newly connected RS232 system will connect and take control of the devices.

8 Files required for Security Escort

The following files must be in the same directory as ESC32.EXE (default “C:\ESCORT”).

Files	Description
Esc32.exe	the main program
Bwcc32.dll	support for the dialog appearance
Cdrvdl32.dll	communications support
Cdrvhf32.dll	communications support
Cdrvxf32.dll	communications support
Commsc32.dll	communications support
W32mkde.exe	the database manager
W32mkrc.dll	support for the database manager
Wbtrcall.dll	support for the database manager
Wbtrv32.dll	support for the database manager
Lfbmp70n.dll	support for the screen images
Lfcmp70n.dll	support for the screen images
Ltkrn70n.dll	support for the screen images
Ltfil70n.dll	support for the screen images

The following files are the preferences for this workstation and are stored in the same directory as ESC32.EXE.

Files	Description
Wprefers.edb	the workstation preferences settings
Prefersc.edb	Old system preferences settings. This file is converted to gprefers.edb and wprefers.edb, and then is automatically deleted.

The map of the facility is a standard Windows bitmap (BMP) file. It must be stored in the same directory as ESC32.EXE.

Files	Description
MAP0.EDB	Main map bitmap file.
MAP1.EDB	Extra map bitmap file if used.
MAP2.EDB	Extra map bitmap file if used.

The following files are the system databases that are stored at the Master Database path (duplicate copy in the Slave Database Path).

Files	Description
Operator.edb	System Operators Database
Preferen.edb	System Preferences settings
Reports.edb	Alarm Reports database
Subscrib.edb	Database of the Subscribers/ Transmitters
Transpon.edb	Database of the System Configuration
Gprefers.edb	Global system preferences settingss

The following sound files should be in the Windows\media directory:

Files	Description
SEtroubl.wav	trouble sound
SEalarm.wav	alarm sound

These are sample images for demo and test. The following files should be in the IMAGES directory, which is a sub-directory to the ESC32.EXE directory (default “C:\ESCORT\IMAGES”)

Files	Description
Image1.jpg	sample subscriber image
Image2.jpg	sample subscriber image
Image3.jpg	sample subscriber image

9 Appendix: Software licenses

This product contains both software that is proprietary Bosch software licensed under the Bosch standard license terms, and software licensed on the basis of other licenses.

9.1 Bosch software

All Bosch software © Bosch Security Systems. Bosch software is licensed under the terms of the End User License Agreement (EULA) of Bosch Security Systems B.V. or Bosch Security Systems Inc, as available together with the physical carrier (CD or DVD). Any use is subject to agreement and compliance with such EULA, as applicable.

9.2 Other licenses – copyright notices

Bosch is committed to comply with the relevant terms of any open source license included in its products. The open source licenses for Security Escort 2.15 are listed in the **OpenSourceLicensing.doc** file in the Open Source folder of the CD-ROM. The relevant open source software or source code can also be obtained by downloading from the Bosch product catalog website.

9.3 Warranties and disclaimer of warranties

Software provided under other licenses has specific disclaimers of warranties. These are repeated in the full license texts, and apply in full to the relevant software components. All software components provided under the other licenses are provided "as is" without any warranty of any kind, including but not limited to any implied warranty of merchantability or fitness for a particular purpose, unless stated otherwise in writing. Please see the full text of the relevant software licenses for further details. The Bosch standard product warranty only applies to the combination of hardware and software as delivered by Bosch. Without prejudice to any licensee's right to apply the provisions of a relevant software license, any modification of any software delivered with or as part of the product may render any warranty on the whole product or any parts thereof null and void, and Bosch is entitled to charge fees for any services in relation thereto.

Index

Robert Bosch (SEA) Pte Ltd
11 Bishan Street 21
573943 Singapore
Singapore
www.boschsecurity.com

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany